vce trainer

Reference Solution for cisa.vce

CISA

CISA

Certified Information Systems Auditor

Version 14.0

Score: 800/1000

Version:

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Exam A (2791 questions)

Question 1

Which of the following BEST describes the relationship between vulnerability scanning and penetration testing?

- ☐ For entities with regulatory drivers the two tests must be the same.
- ☐ Both are labor-intensive in preparation, planning and execution.
- ☒ Both utilize a risk-based analysis that considers treats scenarios.
- ☐ The scope of both is determined primarily by the likelihood of exploitation.

Question 2

During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:

- ☒ the level of information security required when business recovery procedures are invoked.
- ☐ information security roles and responsibilities in the crisis management structure.
- ☐ information security resource requirements.
- ☐ change management procedures for information security that could affect business continuity arrangements.

Explanation:

Explanation:

Business should consider whether information security levels required during recovery should be the same, lower or higher than when business is operating normally. In particular, any special rules for access to confidential data during a crisis need to be identified. The other choices do not directly address the information confidentiality issue.

Question 3

Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?

- ☐ Number of published applications-recovery plans
- ☒ Ratio of successful to unsuccessful tests
- ☐ Ratio of recovery-plan documents to total applications
- ☐ Ratio of tested application to total applications

Licensed to Berend Post berend.post@it-university.nl

Question 4

There are several methods of providing telecommunications continuity. The method of routing traffic through split cable or duplicate cable facilities is called:

- ☐ alternative routing.
- ☒ diverse routing.
- ☐ long-haul network diversity.
- ☐ last-mile circuit protection.

Explanation:

Explanation:

Diverse routing routes traffic through split-cable facilities or duplicate-cable facilities. This can be accomplished with different and/or duplicate cable sheaths, if different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual-entrance facilities. This type of access is time consuming and costly. Alternative routing is a method of routing information via an alternate medium, such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Long-haul network diversity is a diverse, long-distance network utilizing T-l circuits among the major long-distance carriers. It ensures long-distance access should any carrier experience a network failure. Last-mile circuit protection is a redundant combination of local carrier T-ls, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local-carrier routing is also utilized.

Question 5

To restore service at a large processing facility after a disaster, which of the following tasks should be performed FIRST?

- ☒ Launch the emergency action team.
- ☐ Inform insurance company agents.
- ☐ Contact equipment vendors.
- ☐ Activate the reciprocal agreement.

Question 6

Which of the following is the BEST approach to identify whether a vulnerability is actively being exploited?

- ☐ Implement key performance indicators (KPIs).
- ☐ Conduct a penetration test.
- ☐ Review service desk reports.
- ☒ Perform log analysis.

Licensed to Berend Post berend.post@it-university.nl

Question 7

The demilitarized zone (DMZ) is the part of a network where servers that are placed are:

- ☐ running internal department applications.
- ☐ running mission-critical, non-web applications.
- ☒ interacting with the public Internet.
- ☐ external to the organization.

Question 8

Which of the following should an IS auditor recommend be done FIRST upon learning that new data protection legislation may affect the organization?

- ☐ Implement data protection best practices
- ☐ Implement a new security baseline for achieving compliance
- ☐ Restrict system access for noncompliant business processes
- ☒ Perform a gap analysis of data protection practices

Question 9

Which of the following needs be established FIRST in order to categorize data properly?

- ☐ A data protection policy
- ☒ A data classification framework
- ☐ A data asset inventory
- ☐ A data asset protection standard

Question 10

An IS auditor should ensure that an application's audit trail:

- ☐ has adequate security
- ☒ does not impact operational efficiency.
- ☐ is accessible online.
- ☐ logs all database records.

Question 11

You may reduce a cracker's chances of success by (choose all that apply):

- ☒ keeping your systems up to date using a security scanner.
- ☒ hiring competent people responsible for security to scan and update your systems.
- ☐ using multiple firewalls.
- ☐ using multiple firewalls and IDS.
- ☐ None of the choices.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Only a small fraction of computer program code is mathematically proven, or even goes through comprehensive information technology audits or inexpensive but extremely valuable computer security audits, so it is quite possible for a determined cracker to read, copy, alter or destroy data in well secured computers, albeit at the cost of great time and resources. You may reduce a cracker's chances by keeping your systems up to date, using a security scanner or/and hiring competent people responsible for security.

Question 12

Which of the following statement correctly describes one way SSL authentication between a client (e.g. browser) and a server (e.g. web server)?

- ☒ Only the server is authenticated while client remains unauthenticated
- ☐ Only the client is authenticated while server remains authenticated
- ☐ Client and server are authenticated
- ☐ Client and server are unauthenticated

Explanation:

In one way authentication only server needs to be authenticated where as in mutual authentication both the client and the server needs to be authenticated.

For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)

These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases

Peer negotiation for algorithm support

Public-key, encryption based key exchange and certificate based authentication

Symmetric cipher based traffic encryption.

Licensed to Berend Post berend.post@it-university.nl

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

The other choices presented in the options are not valid as in one way authentication only server needs to be authenticated where as client will remain unauthenticated.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352

Question 13

What would be an IS auditor's GREATEST concern when using a test environment for an application audit?

- ☐ Test and production environments lack data encryption.
- ☐ Developers have access to the test environment.
- ☐ Retention period of test data has been exceeded.
- ☒ Test and production environments do not mirror each other.

Question 14

Which of the following is appropriate when an IS auditor is conducting an exit meeting with senior management?

- ☐ Eliminate significant findings where audit and management agree on risk acceptance.
- ☐ Agree with senior management on the risk grading of the audit report.
- ☒ Document written responses from management along with an implementation plan.
- ☐ Escalate disputed recommendations to the audit committee.

Licensed to Berend Post berend.post@it-university.nl

Question 15

Which of the following controls is MOST appropriate against brute force attacks at login?

- ☐ Storing password files using one-way encryption
- ☒ Locking the account after three invalid passwords
- ☐ Storing passwords under a one-way hash function
- ☐ Increasing the minimum password length to 10 characters

Question 16

Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

- ☐ Bottom up
- ☐ Sociability testing
- ☒ Top-down
- ☐ System test

Explanation:

Explanation:

The top-down approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early. A bottom-up approach to testing begins with atomic units, such as programs and modules, and works upward until a complete system test has taken place. Sociability testing and system tests take place at a later stage in the development process.

Question 17

Which of the following would MOST likely impact the integrity of a database backup?

- ☐ Record fields contain null information
- ☐ Open database files during backup
- ☐ Relational database model used
- ☒ Backing up the database to an optical disk

Question 18

Which of the following security processes will BEST prevent the exploitation of system vulnerabilities?

- ☒ Patch management
- ☐ Log monitoring
- ☐ Antivirus software
- ☐ Intrusion detection

Licensed to Berend Post berend.post@it-university.nl

Question 19

Which of the following technique is used for speeding up network traffic flow and making it easier to manage?

- ☐ Point-to-point protocol
- ☐ X.25
- ☒ MPLS
- ☐ ISDN

Explanation:

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

For your exam you should know below information about WAN Technologies:

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Licensed to Berend Post berend.post@it-university.nl

Point-to-point protocol

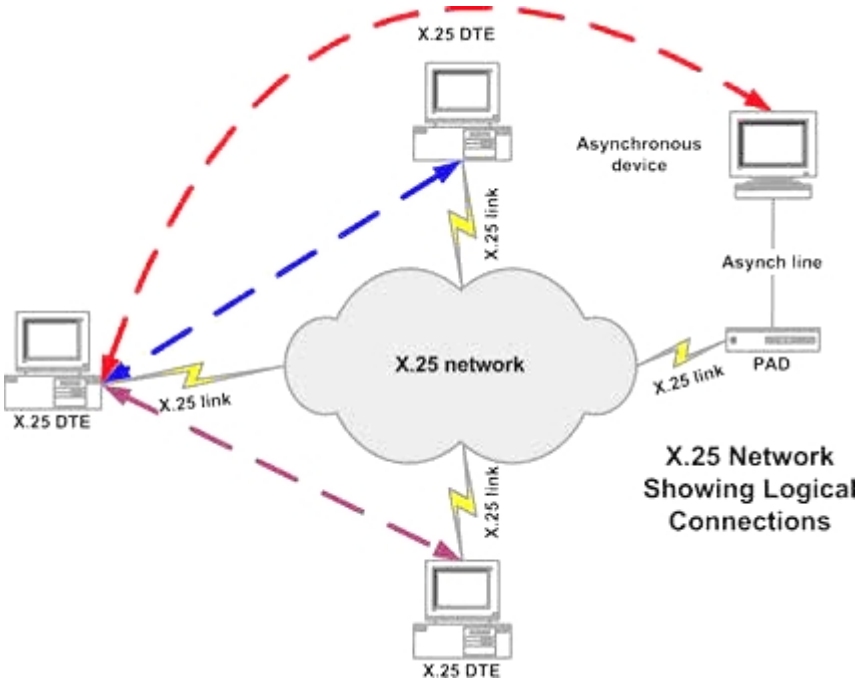
X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.



X.25

Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Licensed to Berend Post berend.post@it-university.nl

Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.

ISDN

Asynchronous Transfer Mode (ATM)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

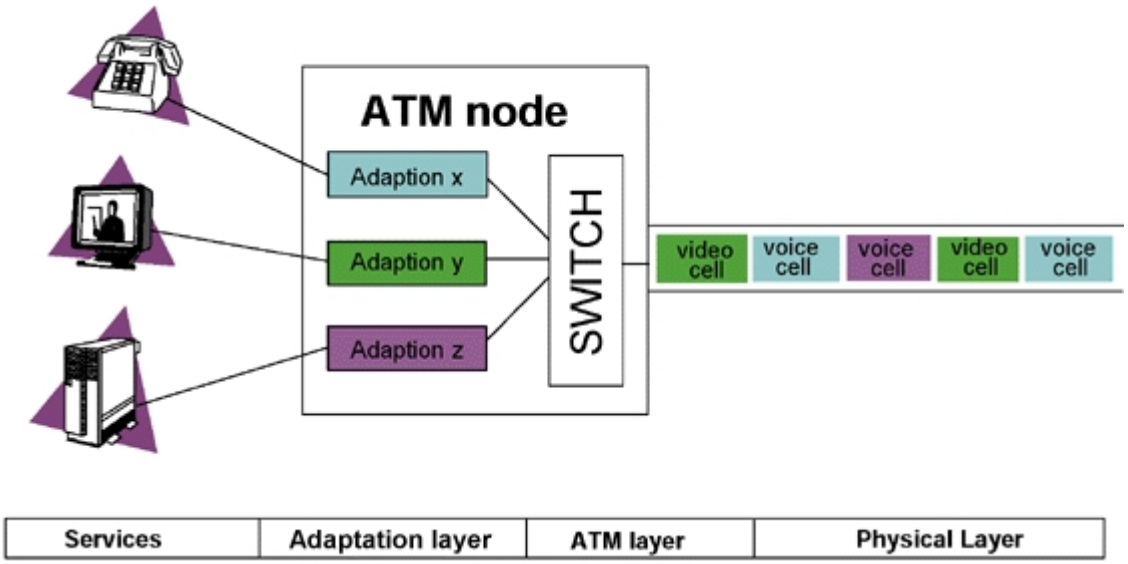
Like a frame relay it is connection oriented technology which creates and uses fixed channel

Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM

Asynchronous Transfer Mode

 Licensed to Berend Post berend.post@it-university.nl

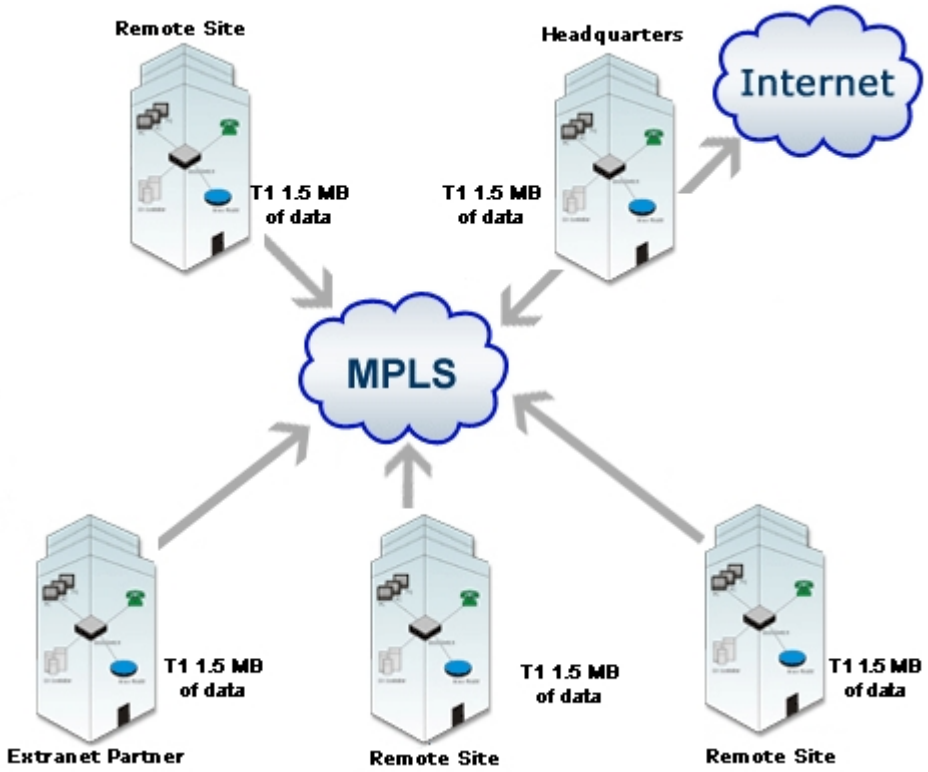


Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS

Licensed to Berend Post berend.post@it-university.nl



The following answers are incorrect:

X.25 - X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Point-to-point protocol - PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.

ISDN -Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

Licensed to Berend Post berend.post@it-university.nl

Question 20

An IS auditor determines that an online retailer processing credit card information does not have a data classification process. The auditor's NEXT step should be to:

- ☐ recommend encryption of all sensitive data at rest
- ☒ determine existing controls around sensitive data
- ☐ recommend the implementation of data loss prevention (DLP) tools
- ☐ inquire if there have been any data loss incidents

Question 21

Which of the following is the BEST approach to verify that internal help desk procedures are executed in compliance with policies?

- ☐ Benchmark help desk procedures.
- ☐ Interview end users.
- ☐ Test a sample of closed tickets.
- ☒ Evaluate help desk call metrics.

Question 22

Which should be reviewed FIRST by an IS auditor to ensure that data is being secured appropriately for an application?

- ☒ Data classification
- ☐ Data encryption
- ☐ Data access
- ☐ Data storage

Explanation:

Explanation:

Data classification is necessary to provide proper access rights to the users. If you do not classify data according to their sensitivity and importance to the business, you cannot apply proper access rules to them. Data owners are responsible for defining access rules. The data classification process starts with the process of establishing ownership of data. This process also helps to prepare data dictionary

Question 23

An information security manager reads a media report of a new type of malware attack. Who should be notified FIRST?

- ☒ Security operations team
- ☐ Data owners
- ☐ Communications department
- ☐ Application owners

Licensed to Berend Post berend.post@it-university.nl

Question 24

When using public key encryption to secure data being transmitted across a network:

- ☐ both the key used to encrypt and decrypt the data are public.
- ☐ the key used to encrypt is private, but the key used to decrypt the data is public.
- ☒ the key used to encrypt is public, but the key used to decrypt the data is private.
- ☐ both the key used to encrypt and decrypt the data are private.

Explanation:

Explanation:

Public key encryption, also known as asymmetric key cryptography, uses a public key to encrypt the message and a private key to decrypt it.

Question 25

An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

- ☐ Design further tests of the calculations that are in error.
- ☐ Identify variables that may have caused the test results to be inaccurate.
- ☒ Examine some of the test cases to confirm the results.
- ☐ Document the results and prepare a report of findings, conclusions and recommendations.

Explanation:

Explanation:

An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would not be made until all results are confirmed.

Question 26

Which of the following procedures should be implemented prior to disposing of surplus computer equipment to employees?

- ☐ Use operating system commands to delete all files from the hard drive.
- ☐ Have the employee receiving the machine sign a nondisclosure agreement.
- ☐ Use application delete commands to remove files.
- ☒ Overwrite the hard drive with random data.

Licensed to Berend Post berend.post@it-university.nl

Question 27

Which of the following layer of the OSI model provides a standard interface for applications to communicate with devices on a network?

- ☒ Application layer
- ☐ Presentation layer
- ☐ Session layer
- ☐ Transport layer

Explanation:

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

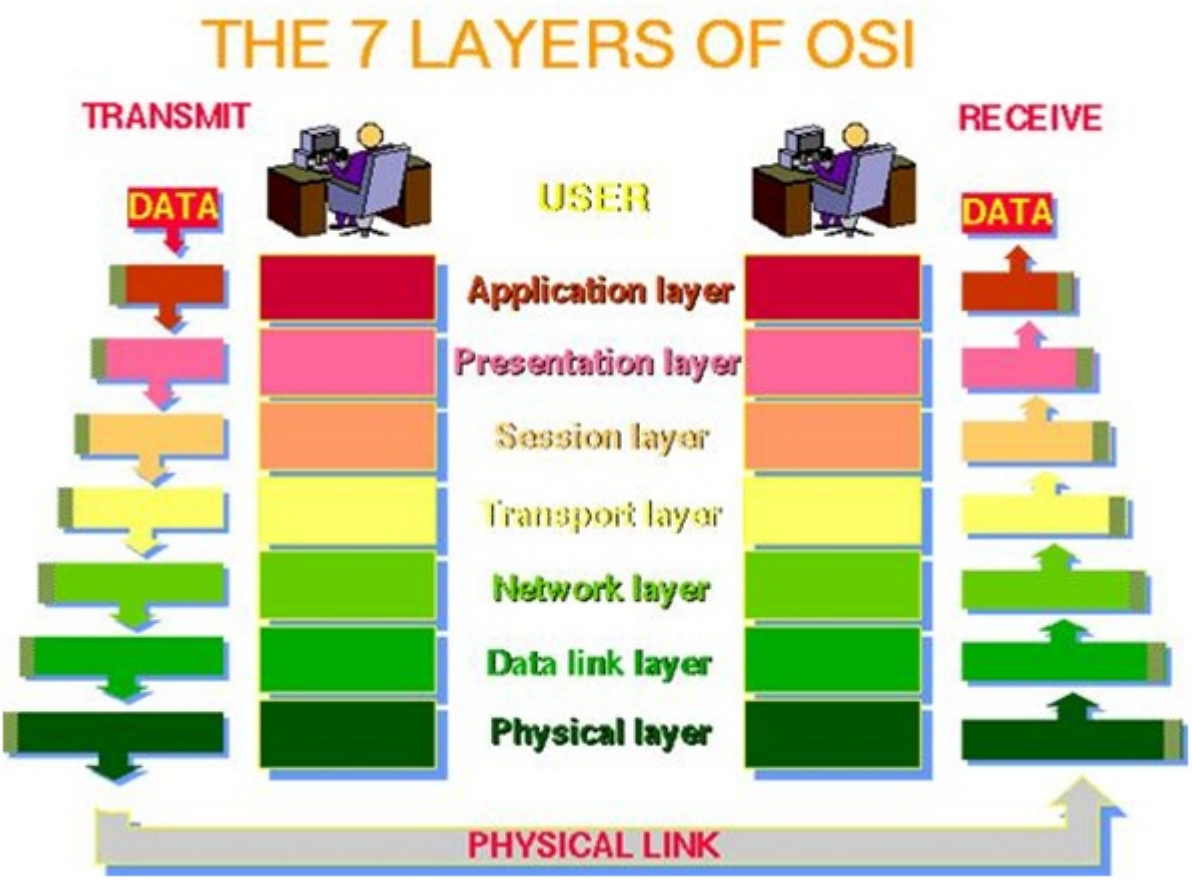
For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model

Licensed to Berend Post berend.post@it-university.nl



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Licensed to Berend Post berend.post@it-university.nl

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

Licensed to Berend Post berend.post@it-university.nl

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

Licensed to Berend Post berend.post@it-university.nl

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used

Licensed to Berend Post berend.post@it-university.nl

by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Session layer - The session layer allows session establishment between processes running on different stations.

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Question 28

The CIO of an organization is concerned that the information security policies may not be comprehensive. Which of the following should an IS auditor recommend be performed FIRST?

- ☐ Obtain a copy of their competitor's policies.
- ☐ Determine if there is a process to handle exceptions to the policies.
- ☒ Establish a governance board to track compliance with the policies.
- ☐ Compare the policies against an industry framework.

Question 29

Which of the following attack could be avoided by creating more security awareness in the organization and provide adequate security knowledge to all employees?

- ☐ surf attack
- ☐ Traffic analysis
- ☒ Phishing
- ☐ Interrupt attack

Explanation:

Phishing techniques include social engineering, link manipulation, spear phishing, whaling, dishing, or web site forgery techniques.

For your exam you should know the information below:

Licensed to Berend Post berend.post@it-university.nl

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

Smurf Attack – Occurs when mix-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 323

Official ISC2 guide to CISSP CBK 3rd Edition Page number 493

http://en.wikipedia.org/wiki/Phishing

Question 30

Which of the following findings should be an IS auditor's GREATEST concern when reviewing an organization's purchase of new IT infrastructure hardware?

- ☐ The new infrastructure arrived with default system settings.
- ☐ The new infrastructure has residual risk within the organization's risk tolerance.
- ☐ The new infrastructure's hardening requirements are stronger than required by policy.
- ☒ The new infrastructure has compatibility issues with existing systems.

Question 31

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

- ☐ Mobile
- ☒ Redundant
- ☐ Shared
- ☐ Warm

Licensed to Berend Post berend.post@it-university.nl

Question 32

Which of the following database controls would ensure that the integrity of transactions is maintained in an online transaction processing system's database?

- ☐ Authentication controls
- ☐ Data normalization controls
- ☐ Read/write access log controls
- ☒ Commitment and rollback controls

Explanation:

Explanation:

Commitment and rollback controls are directly relevant to integrity. These controls ensure that database operations that form a logical transaction unit will complete in its entirety or not at all; i.e., if, for some reason, a transaction cannot be fully completed, then incomplete inserts/updates/deletes are rolled back so that the database returns to its pretransaction state. All other choices would not address transaction integrity.

Question 33

When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

- ☐ Before transaction completion
- ☐ Immediately after an EFT is initiated
- ☐ During run-to-run total testing
- ☒ Before an EFT is initiated

Explanation:

Explanation:

An application-level edit check to verify availability of funds should be completed at the electronic funds transfer (EFT) interface before an EFT is initiated.

Question 34

Which of the following is the PRIMARY reason for database optimization in an environment with a high volume of transactions?

- ☐ Improving availability
- ☐ Maintaining integrity
- ☐ Preventing data leakage
- ☒ Improving performance

Licensed to Berend Post berend.post@it-university.nl

Question 35

Which of the following refers to a primary component of corporate risk management with the goal of minimizing the risk of prosecution for software piracy due to use of unlicensed software?

- ☒ Software audit
- ☐ System audit
- ☐ Application System audit
- ☐ Test audit
- ☐ Mainframe audit
- ☐ None of the choices.

Explanation:

Explanation:

Software audits are a component of corporate risk management, with the goal of minimizing the risk of prosecution for software piracy due to use of unlicensed software. From time to time internal or external audits may take a forensic approach to establish what is installed on the computers in an organization with the purpose of ensuring that it is all legal and authorized and to ensure that its process of processing transactions or events is correct.

Question 36

The GREATEST risk when performing data normalization is:

- ☒ the increased complexity of the data model
- ☐ duplication of audit logs
- ☐ reduced data redundancy
- ☐ decreased performance

Question 37

Which of the following BEST reduces the likelihood of leakage of private information via email?

- ☐ Strong user authentication protocols
- ☐ Email encryption
- ☐ Prohibition on the personal use of email
- ☒ User awareness training

Question 38

Which of the following protocol is used for electronic mail service?

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☒ SMTP

Explanation:

Licensed to Berend Post berend.post@it-university.nl

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

For your exam you should know below information general Internet terminology:

Network access point -Internet service providers access internet using net access point. A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Licensed to Berend Post berend.post@it-university.nl

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:

DNS - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three

 Licensed to Berend Post berend.post@it-university.nl

utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 273 and 274

Question 39

Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

- ☒ Data diddling
- ☐ Skimming
- ☐ Data corruption
- ☐ Salami attack

Explanation:

Explanation:

Data diddling involves modifying data before or during systems data entry.

Question 40

Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

- ☐ Review software migration records and verify approvals.
- ☒ identify changes that have occurred and verify approvals.
- ☐ Review change control documentation and verify approvals.
- ☐ Ensure that only appropriate staff can migrate changes into production.

Explanation:

Explanation:

The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

Licensed to Berend Post berend.post@it-university.nl

Question 41

Which of the following will BEST ensure the successful offshore development of business applications?

- ☐ Stringent contract management practices
- ☒ Detailed and correctly applied specifications
- ☐ Awareness of cultural and political differences
- ☐ Post implementation reviews

Explanation:

Explanation:

When dealing with offshore operations, it is essential that detailed specifications be created. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptions and modifications may not be adequately communicated. Contract management practices, cultural and political differences, and post implementation reviews, although important, are not as pivotal to the success of the project.

Question 42

With Deep packet inspection, which of the following OSI layers are involved?

- ☒ Layer 2 through Layer 7
- ☐ Layer 3 through Layer 7
- ☐ Layer 2 through Layer 6
- ☐ Layer 3 through Layer 6
- ☐ Layer 2 through Layer 5
- ☐ None of the choices.

Explanation:

Explanation:

Deep packet inspection (DPI) is a form of computer network packet filtering that examines the data part of a through-passing packet, searching for non- protocol compliance or predefined criteria to decide if the packet can pass.

DPI devices have the ability to look at Layer 2 through Layer 7 of the OSI model.

Licensed to Berend Post berend.post@it-university.nl

Question 43

An IS auditor reviewing an incident management process identifies client information was lost due to ransomware attacks. Which of the following would MOST effectively minimize the impact of future occurrences?

- ☐ Change access to client data to read-only.
- ☒ Improve the ransomware awareness program.
- ☐ Back up client data more frequently.
- ☐ Monitor all client data changes.

Question 44

What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources?

- ☐ OSI Layer 2 switches with packet filtering enabled
- ☐ Virtual Private Networks
- ☒ Access Control Lists (ACL)
- ☐ Point-to-Point Tunneling Protocol

Explanation:

Explanation:

ISPs can use access control lists to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources.

Question 45

IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- ☒ desired result or purpose of implementing specific control procedures.
- ☐ best IT security control practices relevant to a specific entity.
- ☐ techniques for securing information.
- ☐ security policy.

Explanation:

Explanation:

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

Licensed to Berend Post berend.post@it-university.nl

Question 46

Who is responsible for providing technical support for the hardware and software environment by developing, installing and operating the requested system?

- ☒ System Development Management
- ☐ Quality Assurance
- ☐ User Management
- ☐ Senior Management

Explanation:

System Development Management provides technical support for hardware and software environment by developing, installing and operating the requested system.

For the CISA exam you should know the information below about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management - Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?

How reliable is the software?

How effective is the software?

Is the software easy to use?

How easy is to transfer or adapt old data from preexisting software to this environment?

Is it possible to add new functions?

Does it meet regulatory requirement?

Project Steering Committee - Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

Licensed to Berend Post berend.post@it-university.nl

System Development Management -Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager -Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor - Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team -Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team -Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the

 Licensed to Berend Post berend.post@it-university.nl

quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

User Management -Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 150

Question 47

The logical exposure associated with the use of a checkpoint restart procedure is:

- ☐ denial of service.
- ☒ an asynchronous attack
- ☐ wire tapping.
- ☐ computer shutdown.

Explanation:

Explanation:

Asynchronous attacks are operating system-based attacks. A checkpoint restart is a feature that stops a program at specified intermediate points for later restart in an orderly manner without losing data at the checkpoint. The operating system saves a copy of the computer programs and data in their current state as well as several system parameters describing the mode and security level of the program at the time of stoppage. An asynchronous attack occurs when an individual with access to this information is able to gain access to the checkpoint restart copy of the system parameters and change those parameters such that upon restart the program would function at a higher-priority security level.

Licensed to Berend Post berend.post@it-university.nl

Question 48

Which of the following is the BEST compensating control for a lack of proper segregation of duties in an IT department?

- ☐ Authorization forms
- ☐ Audit trail reviews
- ☒ System activity logging
- ☐ Control self-assessment (CSA)

Question 49

At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

- ☐ report the error as a finding and leave further exploration to the auditee's discretion.
- ☐ attempt to resolve the error.
- ☒ recommend that problem resolution be escalated.
- ☐ ignore the error, as it is not possible to get objective evidence for the software error.

Explanation:

Explanation:

When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

Question 50

The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

- ☐ prevent omission or duplication of transactions.
- ☐ ensure smooth data transition from client machines to servers.
- ☐ ensure that e-mail messages have accurate time stamps.
- ☒ support the incident investigation process.

Explanation:

Explanation:

During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult because a time line of events might not be easily established. Time-stamping a transaction has nothing to do with the update itself. Therefore, the possibility of omission or duplication of transactions does not exist. Data transfer has nothing to do with the time stamp. While the time stamp on an e-mail may not be accurate, this is not a significant issue.

Licensed to Berend Post berend.post@it-university.nl

Question 51

Which of the following is the MOST effective way for an organization to protect against data leakage?

- ☐ Conduct periodic security awareness training.
- ☐ Limit employee Internet access.
- ☐ Review firewall logs for anomalies.
- ☒ Develop a comprehensive data loss prevention policy.

Question 52

After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- ☐ Project management and progress reporting is combined in a project management office which is driven by external consultants.
- ☒ The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach.
- ☐ The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy systems.
- ☐ The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training needs.

Explanation:

Explanation:

The efforts should be consolidated to ensure alignment with the overall strategy of the post-merger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In post-merger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralize dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. Itis a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

Licensed to Berend Post berend.post@it-university.nl

Question 53

An IS auditor will be testing accounts payable controls by performing data analytics on the entire population transactions. Which of the following is MOST important for the auditor to confirm when sourcing the population data?

- ☒ There is no privacy information in the data.
- ☐ The data analysis tools have been recently updated.
- ☐ The data can be obtained in a timely manner.
- ☐ The data is taken directly from the system.

Question 54

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- ☒ effectiveness of the QA function because it should interact between project management and user management
- ☐ efficiency of the QA function because it should interact with the project implementation team.
- ☐ effectiveness of the project manager because the project manager should interact with the QA function.
- ☐ efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Explanation:

Explanation:

To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness. The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

Question 55

From a control perspective, the key element in job descriptions is that they:

- ☐ provide instructions on how to do the job and define authority.
- ☐ are current, documented and readily available to the employee.
- ☐ communicate management's specific job performance expectations.
- ☒ establish responsibility and accountability for the employee's actions.

Explanation:

Explanation:

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job

Licensed to Berend Post berend.post@it-university.nl

responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

Question 56

Which of the following statement INCORRECTLY describes packet switching technique?

- ☐ Packet uses many different dynamic paths to get the same destination
- ☐ Traffic is usually burst in nature
- ☒ Fixed delays to reach each packet to destination
- ☐ Usually carries data-oriented data

Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about packet switching. As in the network switching, packet traverse different path, there will be always variable delay for each packet to reach to destination.

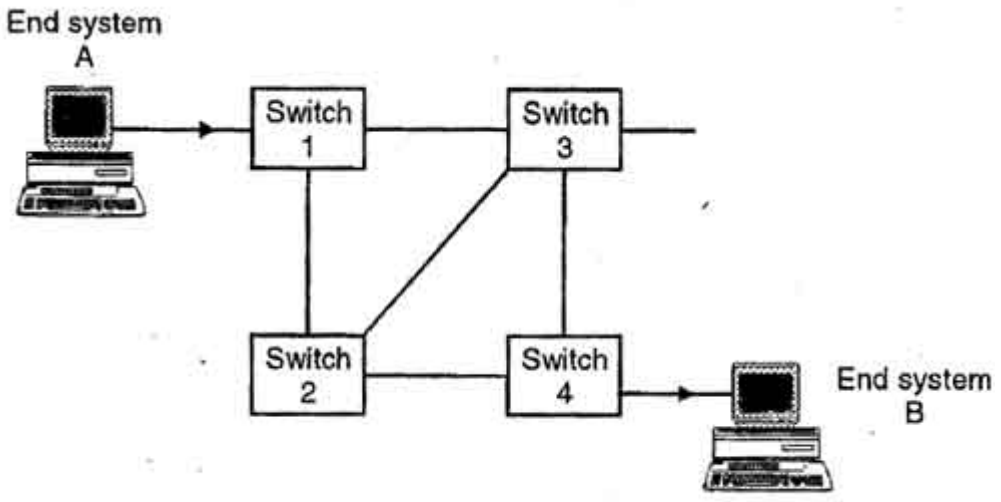
For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

 Licensed to Berend Post berend.post@it-university.nl

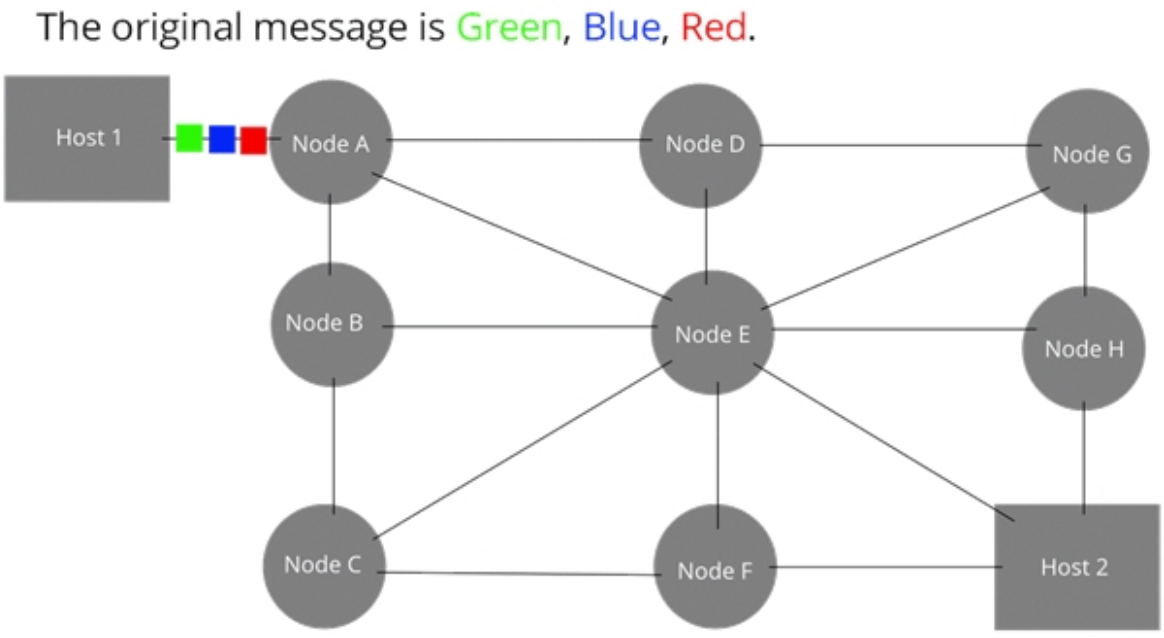


Message switched data network

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching



Circuit Switching

Licensed to Berend Post berend.post@it-university.nl

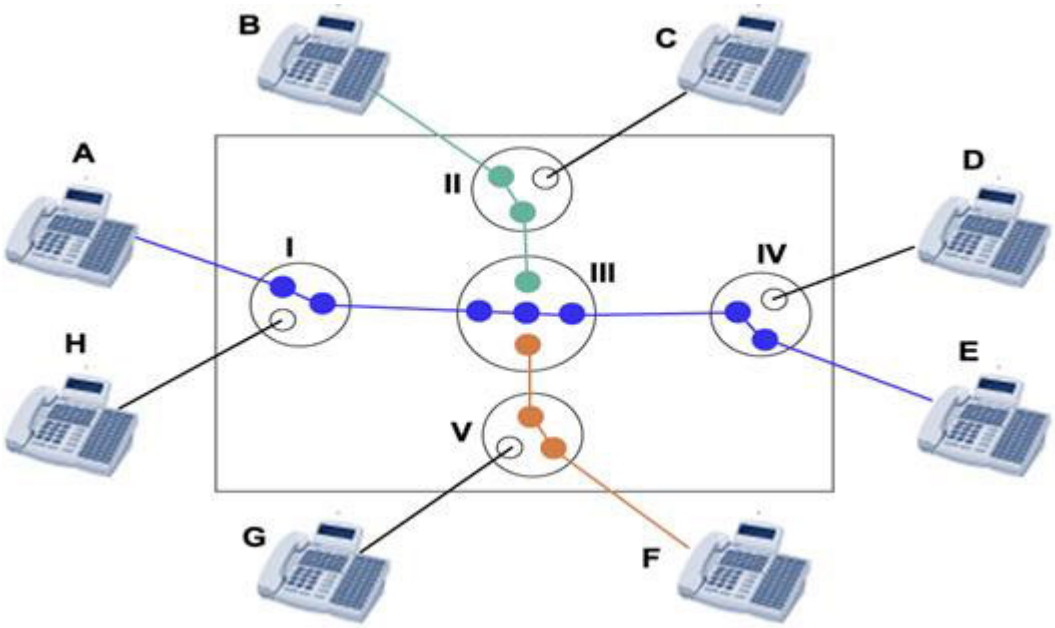
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching



See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

Licensed to Berend Post berend.post@it-university.nl

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented correctly describes about packet switching.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

Licensed to Berend Post berend.post@it-university.nl

Question 57

Which of the following cryptography options would increase overhead/cost?

- ☐ The encryption is symmetric rather than asymmetric.
- ☒ A long asymmetric encryption key is used.
- ☐ The hash is encrypted rather than the message.
- ☐ A secret key is used.

Explanation:

Explanation:

Computer processing time is increased for longer asymmetric encryption keys, and the increase may be disproportionate. For example, one benchmark showed that doubling the length of an RSA key from 512 bits to 1,024 bits caused the decrypt time to increase nearly six-fold. An asymmetric algorithm requires more processing time than symmetric algorithms. A hash is shorter than the original message; therefore, a smaller overhead is required if the hash is encrypted rather than the message. Use of a secret key, as a symmetric encryption key, is generally small and used for the purpose of encrypting user data.

Question 58

Management decided to accept the residual risk of an audit finding and not take the recommended actions. The internal audit team believes the acceptance is inappropriate and has discussed the situation with executive management. After this discussion, there is still disagreement regarding the decision. Which of the following is the BEST course of action by internal audit?

- ☐ Report this matter to the audit committee without notifying executive management.
- ☐ Document in the audit report that management has accepted the residual risk and take no further actions.
- ☒ Report the issue to the audit committee in a joint meeting with executive management for resolution.
- ☐ Schedule another meeting with executive management to convince them of taking action as recommended.

Question 59

An IS auditor intends to accept a management position in the data processing department within the same organization. However, the auditor is currently working on an audit of a major application and has not yet finished the report. Which of the following would be the BEST step for the IS auditor to take?

- ☐ Start in the position and inform the application owner of the job change.
- ☐ Start in the position immediately.
- ☒ Disclose this issue to the appropriate parties.
- ☐ Complete the audit without disclosure and then start in the position.

Licensed to Berend Post berend.post@it-university.nl

Question 60

What is the GREATEST concern for an IS auditor reviewing contracts for licensed software that executes a critical business process?

- ☐ Software escrow was not negotiated.
- ☐ An operational level agreement (OLA) was not negotiated.
- ☒ The contract does not contain a right-to-audit clause.
- ☐ Several vendor deliverables missed the commitment date.

Question 61

Which of the following is the GREATEST risk associated with in-house program development and customization?

- ☐ The lack of a test environment
- ☒ The lack of a quality assurance function
- ☐ The lack of secure coding expertise
- ☐ The lack of documentation for programs developed.

Question 62

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. To ensure that management concerns are addressed, which data set should internal audit recommend be reviewed FIRST?

- ☒ Data impacting business objectives
- ☐ Data supporting financial statements
- ☐ Data reported to the regulatory body
- ☐ Data with customer personal information

Question 63

Which of the following would represent an acceptable test of an organization's business continuity plan (BCP)?

- ☐ Benchmarking the plan against similar organizations
- ☐ Paper test involving functional areas
- ☒ Full test of computer operations at an emergency site
- ☐ Walk-through of the plan with technology suppliers

Licensed to Berend Post berend.post@it-university.nl

Question 64

The PRIMARY benefit of a centralized time server is that it:

- ☐ reduces individual time-of-day requests by client applications
- ☐ is required by password synchronization programs
- ☒ allows decentralized logs to be kept in synchronization
- ☐ decreases the likelihood of an unrecoverable systems failure

Question 65

The success of control self-assessment (CSA) highly depends on:

- ☒ having line managers assume a portion of the responsibility for control monitoring.
- ☐ assigning staff managers the responsibility for building, but not monitoring, controls.
- ☐ the implementation of a stringent control policy and rule-driven controls.
- ☐ the implementation of supervision and the monitoring of controls of assigned duties.

Explanation:

Explanation:

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on the degree to which line managers assume responsibility for controls- Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

Question 66

While planning an audit, an assessment of risk should be made to provide:

- ☒ reasonable assurance that the audit will cover material items.
- ☐ definite assurance that material items will be covered during the audit work.
- ☐ reasonable assurance that all items will be covered by the audit.
- ☐ sufficient assurance that all items will be covered during the audit work.

Explanation:

Explanation:

The ISACA IS Auditing Guideline G15 on planning the IS audit states, 'An assessment of risk should be made to provide reasonable assurance that material items will be adequately covered during the audit work. This assessment should identify areas with a relatively high risk of the existence of material problems.' Definite assurance that material items will be covered during the audit work is an impractical proposition. Reasonable assurance that all items will be covered during the audit work is not the correct answer, as material items need to be covered, not all items.

Licensed to Berend Post berend.post@it-university.nl

Question 67

Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

- ☒ A neural network
- ☐ Database management software
- ☐ Management information systems
- ☐ Computer assisted audit techniques

Explanation:

Explanation:

A neural network will monitor and learn patterns, reporting exceptions for investigation.

Question 68

During an audit, the IS auditor finds that in many cases excessive rights were not removed from a system. Which of the following would be the auditor's BEST recommendation?

- ☐ IT security should regularly revoke excessive system rights.
- ☐ System administrators should ensure consistency of assigned rights.
- ☐ Line management should regularly review and request modification of access rights.
- ☒ Human resources should delete access rights of terminated employees.

Question 69

Which of the following is the MOST critical step prior to performing a network penetration test?

- ☒ Informing management of the potential risk involved with penetration testing
- ☐ Identifying a scanning tool for use in identifying vulnerabilities
- ☐ Communicating the location of the penetration test targets to management
- ☐ Reviewing the results of previous penetration tests

Question 70

The BEST method for assessing the effectiveness of a business continuity plan is to review the:

- ☐ plans and compare them to appropriate standards.
- ☒ results from previous tests.
- ☐ emergency procedures and employee training.
- ☐ offsite storage and environmental controls.

Explanation:

Explanation:

Previous test results will provide evidence of the effectiveness of the business continuity plan. Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness. Reviewing emergency

Licensed to Berend Post berend.post@it-university.nl

procedures, offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

Question 71

While reviewing the project plan for a new system prior to go-live, an IS auditor notes that the project team has not documented a fallback plan. Which of the following would be the BEST go-live approach in this situation?

- ☒ Parallel processing
- ☐ Immediate cutover
- ☐ Real-time replication
- ☐ Load balancing

Question 72

To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) in order to determine:

- ☐ the business processes that generate the most financial value for the organization and therefore must be recovered first.
- ☐ the priorities and order for recovery to ensure alignment with the organization's business strategy.
- ☒ the business processes that must be recovered following a disaster to ensure the organization's survival.
- ☐ he priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

Explanation:

Explanation:

To ensure the organization's survival following a disaster, it is important to recover the most critical business processes first, it is a common mistake to overemphasize value (A) rather than urgency. For example, while the processing of incoming mortgage loan payments is important from a financial perspective, it could be delayed for a few days in the event of a disaster. On the other hand, wiring funds to close on a loan, while not generating direct revenue, is far more critical because of the possibility of regulatory problems, customer complaints and reputation issues. Choices B and D are not correct because neither the long-term business strategy nor the mere number of recovered systems has a direct impact at this point in time.

Licensed to Berend Post berend.post@it-university.nl

Question 73

Which of the following is MOST important for an effective control self-assessment program?

- ☐ Determining the scope of the assessment
- ☐ Evaluating changes to the risk environment
- ☒ Understanding the business process
- ☐ Performing detailed test procedures

Question 74

A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual's experience and:

- ☐ length of service, since this will help ensure technical competence.
- ☐ age, as training in audit techniques may be impractical.
- ☐ IS knowledge, since this will bring enhanced credibility to the audit function.
- ☒ ability, as an IS auditor, to be independent of existing IS relationships.

Explanation:

Explanation:

Independence should be continually assessed by the auditor and management. This assessment should consider such factors as changes in personal relationships, financial interests, and prior job assignments and responsibilities. The fact that the employee has worked in IS for many years may not in itself ensure credibility. The audit department's needs should be defined and any candidate should be evaluated against those requirements. The length of service will not ensure technical competency. Evaluating an individual's qualifications based on the age of the individual is not a good criterion and is illegal in many parts of the world.

Question 75

Which of the following should be the PRIMARY basis for prioritizing follow-up audits?

- ☐ Complexity of management's actions plans
- ☐ Recommendation from executive management
- ☐ Audit cycle defined in the audit plan
- ☒ Residual risk from the findings of previous audits

Licensed to Berend Post berend.post@it-university.nl

Question 76

Which of the following is the MOST appropriate responsibility of an IS auditor involved in a data center renovation project?

- ☒ Performing independent reviews of responsible parties engaged in the project
- ☐ Ensuring the project progresses as scheduled and milestones are achieved
- ☐ Performing day-to-day activities to ensure the successful completion of the project
- ☐ Providing sign off on the design of controls for the data center

Question 77

When auditing a quality assurance plan, an IS auditor should be MOST concerned if the:

- ☐ quality assurance function is separate from the programming function.
- ☐ SDLC is coupled with the quality assurance plan.
- ☐ quality assurance function is periodically reviewed by internal audit.
- ☒ scope of quality assurance activities is undefined.

Question 78

An audit team has a completed schedule approved by the audit committee. After starting some of the scheduled audits, executive management asked the team to immediately audit an additional process. There are not enough resources available to add the additional audit to the schedule. Which of the following is the BEST course of action?

- ☐ Revise the scope of scheduled audits.
- ☒ Propose a revised audit schedule.
- ☐ Approve overtime work to ensure the audit is completed.
- ☐ Consider scheduling the audit for the next period.

Question 79

During a vendor management database audit, an IS auditor identifies multiple instances of duplicate vendor records. In order to prevent recurrence of the same issue, which of the following would be the IS auditor's BEST recommendation to management?

- ☒ Perform system verification checks for unique data values on key fields.
- ☐ Request senior management approval of all new vendor details.
- ☐ Run system reports of full vendor listings periodically to identify duplication.
- ☐ Build a segregation of duties control into the vendor creation process.

Licensed to Berend Post berend.post@it-university.nl

Question 80

The information in the knowledge base can be expressed in several ways. Which of the following way uses questionnaires to lead the user through a series of choices until a conclusion is reached?

- ☒ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Knowledge interface

Explanation:

Decision tree uses questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

For CISA Exam you should know below information about Artificial Intelligence and Expert System

Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used

Goals are generated and achieved

Information is communicated

Collaboration is achieved

Concepts are formed

Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.

Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Licensed to Berend Post berend.post@it-university.nl

Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degrees Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

Knowledge interface – Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Rule - Expressing declarative knowledge through the use of if-then relationships.

Semantic nets - Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

Knowledge interface - Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 187

Licensed to Berend Post berend.post@it-university.nl

Question 81

When reviewing an end-user computing (EUC) application, which of the following techniques is MOST appropriate for testing program logic?

- ☒ Integrated testing facility
- ☐ Test decking
- ☐ Re-performance
- ☐ Key calculation inspection

Question 82

An IS auditor doing penetration testing during an audit of internet connections would:

- ☐ evaluate configurations.
- ☐ examine security settings.
- ☐ ensure virus-scanning software is in use.
- ☒ use tools and techniques available to a hacker.

Explanation:

Explanation:

Penetration testing is a technique used to mimic an experienced hacker attacking a live site by using tools and techniques available to a hacker. The other choices are procedures that an IS auditor would consider undertaking during an audit of Internet connections, but are not aspects of penetration testing techniques.

Question 83

To determine who has been given permission to use a particular system resource, an IS auditor should review:

- ☐ activity lists.
- ☒ access control lists.
- ☐ logon ID lists.
- ☐ password lists.

Explanation:

Explanation:

Access control lists are the authorization tables that document the users who have been given permission to use a particular system resource and the types of access they have been granted. The other choices would not document who has been given permission to use (access) specific system resources.

Licensed to Berend Post berend.post@it-university.nl

Question 84

What is the purpose of a hypervisor?

- ☐ Monitoring the performance of virtual machines
- ☐ Cloning virtual machines
- ☐ Deploying settings to multiple machines simultaneously
- ☒ Running the virtual machine environment

Question 85

Which of the following refers to a symmetric key cipher which operates on fixedlength groups of bits with an unvarying transformation?

- ☐ stream cipher
- ☒ block cipher
- ☐ check cipher
- ☐ string cipher
- ☐ None of the choices.

Explanation:

Explanation:

In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation.

A stream cipher, on the other hand, operates on individual digits one at a time.

Question 86

The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

- ☐ Relocate the shut off switch.
- ☒ Install protective covers.
- ☐ Escort visitors.
- ☐ Log environmental failures.

Explanation:

Explanation:

A protective cover over the switch would allow it to be accessible and visible, but would prevent accidental activation.

Licensed to Berend Post berend.post@it-university.nl

Question 87

While observing a full simulation of the business continuity plan, an IS auditor notices that the notification systems within the organizational facilities could be severely impacted by infra structural damage. The BEST recommendation the IS auditor can provide to the organization is to ensure:

- ☐ the salvage team is trained to use the notification system.
- ☐ the notification system provides for the recovery of the backup.
- ☒ redundancies are built into the notification system.
- ☐ the notification systems are stored in a vault.

Explanation:

Explanation:

If the notification system has been severely impacted by the damage, redundancy would be the best control. The salvage team would not be able to use a severely damaged notification system, even if they are trained to use it. The recovery of the backups has no bearing on the notification system and storing the notification system in a vault would be of little value if the building is damaged.

Question 88

Which of the following would be MOST helpful when assessing how applications exchange data with other applications?

- ☐ List of servers and their applications
- ☒ Entity relationship diagram
- ☐ Results of a risk assessment on the applications
- ☐ Configuration management database

Question 89

An IS auditor is conducting a follow-up internal IS audit and determines that several recommendations from the prior year have not been implemented. Which of the following should be the auditor's FIRST course of action?

- ☐ Evaluate the recommendations in context of the current IT environment.
- ☐ Continue the audit and disregard prior audit recommendations.
- ☐ Request management implement recommendations from the prior year.
- ☒ Add unimplemented recommendations as findings for the new audit.

Licensed to Berend Post berend.post@it-university.nl

Question 90

Which of the following is MOST critical to include when developing a data loss prevention (DLP) policy?

- ☐ Identification of the relevant network channels requiring protection
- ☐ Identification of the users, groups and roles to whom the policy will apply
- ☐ Identification of enforcement actions
- ☒ Identification of the content to protect

Question 91

Performance of a biometric measure is usually referred to in terms of (Choose three.):

- ☐ failure to reject rate
- ☒ false accept rate
- ☒ false reject rate
- ☒ failure to enroll rate
- ☐ None of the choices.

Explanation:

Explanation:

Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted in, while the FRR measures the percent of valid users who are wrongly rejected.

Question 92

There are many firewall implementations provided by firewall manufacturers. Which of the following implementation utilize two packet filtering routers and a bastion host? This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ.

- ☐ Dual Homed firewall
- ☒ Screened subnet firewall
- ☐ Screened host firewall
- ☐ Anomaly based firewall

Explanation:

In network security, a screened subnet firewall is a variation of the dual-homed gateway and screened host firewall. It can be used to separate components of the firewall onto separate systems, thereby achieving greater throughput and flexibility, although at some cost to simplicity. As each component system of the screened subnet firewall needs to implement only a specific task, each system is less complex to configure.

A screened subnet firewall is often used to establish a demilitarized zone (DMZ).

Licensed to Berend Post berend.post@it-university.nl

Below are few examples of Firewall implementations:

Screened host Firewall

Utilizing a packet filtering router and a bastion host, this approach implements a basic network layer security and application server security.

An intruder in this configuration has to penetrate two separate systems before the security of the private network can be compromised

This firewall system is configured with the bastion host connected to the private network with a packet filtering router between internet and the bastion host

Dual-homed Firewall

A firewall system that has two or more network interface, each of which is connected to a different network

In a firewall configuration, a dual homed firewall system usually acts to block or filter some or all of the traffic trying to pass between the network

A dual-homed firewall system is more restrictive form of screened-host firewall system

Demilitarize Zone (DMZ) or screened-subnet firewall

Utilizing two packet filtering routers and a bastion host

This approach creates the most secure firewall system since it supports network and application level security while defining a separate DMZ network

Typically, DMZs are configured to limit access from the internet and organization's private network.

The following were incorrect answers:

The other types of firewall mentioned in the option do not utilize two packet filtering routers and a bastion host.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 346

Licensed to Berend Post berend.post@it-university.nl

Question 93

Which of the following situations would increase the likelihood of fraud?

- ☒ Application programmers are implementing changes to production programs.
- ☐ Application programmers are implementing changes to test programs.
- ☐ Operations support staff are implementing changes to batch schedules.
- ☐ Database administrators are implementing changes to data structures.

Explanation:

Explanation:

Production programs are used for processing an enterprise's data. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data. Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of data. The implementation of changes to batch schedules by operations support staff will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

Question 94

Which of the following type of testing has two major categories: QAT and UAT?

- ☐ Interface testing
- ☐ Unit Testing
- ☒ System Testing
- ☐ Final acceptance testing

Question 95

Which of the following would provide the MOST assurance that an application will work in a live environment?

- ☐ Walking through the programs to view the results of error processing
- ☐ Processing of test data to prove that data can be passed between individual programs
- ☐ Walking through the programs to view the results of processing copies of production data.
- ☒ Processing of valid and erroneous data in an acceptance test environment

Licensed to Berend Post berend.post@it-university.nl

Question 96

The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

- ☒ use this information to launch attacks.
- ☐ forward the security alert.
- ☐ implement individual solutions.
- ☐ fail to understand the threat.

Explanation:

Explanation: An organization's computer security incident response team (CSIRT) should disseminate recent threats, security guidelines and security updates to the users to assist them in understanding the security risk of errors and omissions. However, this introduces the risk that the users may use this information to launch attacks, directly or indirectly. An IS auditor should ensure that the CSIRT is actively involved with users to assist them in mitigation of risks arising from security failures and to prevent additional security incidents resulting from the same threat. Forwarding the security alert is not harmful to the organization, implementing individual solutions is unlikely and users failing to understand the threat would not be a serious concern.

Question 97

What can be used to help identify and investigate unauthorized transactions?

- ☐ Postmortem review
- ☐ Reasonableness checks
- ☒ Data-mining techniques
- ☐ Expert systems

Explanation:

Explanation:

Data-mining techniques can be used to help identify and investigate unauthorized transactions.

Question 98

An organization recently experienced a phishing attack that resulted in a breach of confidential information. Which of the following would be MOST relevant for an IS auditor to review when determining the root cause of the incident?

- ☐ Email configurations
- ☒ Simple mail transfer protocol (SMTP) logging
- ☐ Browser configurations
- ☐ Audit logging

Licensed to Berend Post berend.post@it-university.nl

Question 99

While performing a risk-based audit, which of the following would BEST enable an IS auditor to identify and categorize risk?

- ☐ Understanding the control framework
- ☐ Developing a comprehensive risk model
- ☒ Understanding the business environment
- ☐ Adopting qualitative risk analysis

Question 100

When migrating critical systems to a cloud provider, the GREATEST data security concern for an organization would be that data from different clients may be:

- ☐ subject to different service level agreements (SLAs) for disaster recovery.
- ☐ subject to varying government compliance regulations.
- ☒ improperly separated from each other.
- ☐ requested during a legal discovery process.

Question 101

An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

- ☐ Project sponsor
- ☐ System development project team (SPDT)
- ☒ Project steering committee
- ☐ User project team (UPT)

Explanation:

Explanation:

A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

Licensed to Berend Post berend.post@it-university.nl

Question 102

Which of the following would BEST enable effective decision-making?

- ☐ Annualized loss estimates determined from past security events.
- ☐ A universally applied list of generic threats impacts, and vulnerabilities
- ☐ Formalized acceptance of risk analysis by business management
- ☒ A consistent process to analyze new and historical information risk

Question 103

Which of the following validation techniques would BEST prevent duplicate electronic vouchers?

- ☐ Cyclic redundancy check
- ☐ Edit check
- ☒ Reasonableness check
- ☐ Sequence check

Question 104

When auditing a proxy-based firewall, an IS auditor should:

- ☐ verify that the firewall is not dropping any forwarded packets.
- ☐ review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
- ☒ verify that the filters applied to services such as HTTP are effective.
- ☐ test whether routing information is forwarded by the firewall.

Explanation:

Explanation:

A proxy-based firewall works as an intermediary (proxy) between the service or application and the client, it makes a connection with the client and opens a different connection with the server and, based on specific filters and rules, analyzes all the traffic between the two connections.

Unlike a packet-filtering gateway, a proxy-based firewall does not forward any packets. Mapping between media access control (MAC) and IP addresses is a task for protocols such as Address Resolution Protocol/Reverse Address Resolution Protocol (ARP/RARP).

Licensed to Berend Post berend.post@it-university.nl

Question 105

An organization is considering outsourcing the processing of customer insurance claims. An IS auditor notes that customer data will be sent offshore for processing. Which of the following would be the BEST way to address the risk of exposing customer data?

- ☐ Require background checks on all service provider personnel involved in the processing of data.
- ☐ Recommend the use of a service provider within the same country as the organization.
- ☐ Consider whether the service provider has the ability to meet service level agreements (SLAs).
- ☒ Assess whether the service provider meets the organization's data protection policies.

Question 106

Disabling which of the following would make wireless local area networks more secure against unauthorized access?

- ☐ MAC (Media Access Control) address filtering
- ☐ WPA (Wi-Fi Protected Access Protocol)
- ☐ LEAP (Lightweight Extensible Authentication Protocol)
- ☒ SSID (service set identifier) broadcasting

Explanation:

Explanation:

Disabling SSID broadcasting adds security by making it more difficult for unauthorized users to find the name of the access point. Disabling MAC address filtering would reduce security. Using MAC filtering makes it more difficult to access a WLAN, because it would be necessary to catch traffic and forge the MAC address. Disabling WPA reduces security. Using WPA adds security by encrypting the traffic. Disabling LEAP reduces security. Using LEAP adds security by encrypting the wireless traffic.

Question 107

An organization has performance metrics to track how well IT resources are being used, but there has been little progress on meeting the organization's goals. Which of the following would be MOST helpful to determine the underlying reason?

- ☐ Conducting a root cause analysis
- ☐ Re-evaluating organizational goals
- ☒ Re-evaluating key performance indicators (KPIs)
- ☐ Conducting a business impact analysis (BIA)

Licensed to Berend Post berend.post@it-university.nl

Question 108

To install backdoors, hackers generally prefer to use:

- ☒ either Trojan horse or computer worm.
- ☐ either Tripwire or computer virus.
- ☐ either eavedropper or computer worm.
- ☐ either Trojan horse or eavedropper.
- ☐ None of the choices.

Explanation:

Explanation:

A backdoor is a method of bypassing normal authentication procedures.

Many computer manufacturers used to preinstall backdoors on their systems to provide technical support for customers. Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors, hackers prefer to use either Trojan horse or computer worm.

Question 109

Which of the following is critical to the successful establishment of an enterprise IT architecture?

- ☐ A well-defined data migration policy
- ☐ Comparison of the architecture with that of other organizations
- ☐ An architecture encompassing only critical systems
- ☒ Organizational support for standardization

Question 110

Which of the following would help to ensure the portability of an application connected to a database?

- ☐ Verification of database import and export procedures
- ☒ Usage of a structured query language (SQL)
- ☐ Analysis of stored procedures/triggers
- ☐ Synchronization of the entity-relation model with the database physical schema

Explanation:

Explanation:

The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity- relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

Licensed to Berend Post berend.post@it-university.nl

Question 111

The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

- ☐ information assets are overprotected.
- ☐ a basic level of protection is applied regardless of asset value.
- ☒ appropriate levels of protection are applied to information assets.
- ☐ an equal proportion of resources are devoted to protecting all information assets.

Explanation:

Explanation:

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or under protected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

Question 112

The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

- ☐ facilitates user involvement.
- ☐ allows early testing of technical features.
- ☐ facilitates conversion to the new system.
- ☒ shortens the development time frame.

Explanation:

Explanation:

The greatest advantage of RAD is the shorter time frame for the development of a system. Choices A and B are true, but they are also true for the traditional systems development life cycle. Choice C is not necessarily always true.

Question 113

Talking about biometric authentication, which of the following is often considered as a mix of both physical and behavioral characteristics?

- ☒ Voice
- ☐ Finger measurement
- ☐ Body measurement
- ☐ Signature
- ☐ None of the choices.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while behavioral characteristics include signature, gait and typing patterns. Voice is often considered as a mix of both physical and behavioral characteristics.

Question 114

If inadequate, which of the following would be the MOST likely contributor to a denial-of- service attack?

- ☒ Router configuration and rules
- ☐ Design of the internal network
- ☐ Updates to the router system software
- ☐ Audit testing and review techniques

Explanation:

Explanation:

Inadequate router configuration and rules would lead to an exposure to denial-of-service attacks. Choices B and C would be lesser contributors. Choice D is incorrect because audit testing and review techniques are applied after the fact.

Question 115

A benefit of quality of service (QoS) is that the:

- ☐ entire network's availability and performance will be significantly improved.
- ☐ telecom carrier will provide the company with accurate service-level compliance reports.
- ☒ participating applications will have guaranteed service levels.
- ☐ communications link will be supported by security controls to perform secure online transactions.

Explanation:

Explanation:

The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

Licensed to Berend Post berend.post@it-university.nl

Question 116

Which of the following is MOST important when an incident may lead to prosecution?

- ☐ Impact analysis
- ☐ Timely incident detection
- ☐ Independent assessment
- ☒ Preservation of evidence

Question 117

When reviewing a digital certificate verification process, which of the following findings represents the MOST significant risk?

- ☐ There is no registration authority (RA) for reporting key compromises
- ☒ The certificate revocation list(CRL) is not current.
- ☐ Digital certificates contain a public key that is used to encrypt messages and verify digital signatures.
- ☐ Subscribers report key compromises to the certificate authority (CA).

Explanation:

Explanation:

If the certificate revocation list (CRL) is not current, there could be a digital certificate that is not revoked that could be used for unauthorized or fraudulent activities. The certificate authority (CA) can assume the responsibility if there is no registration authority (RA). Digital certificates containing a public key that is used to encrypt messages and verifying digital signatures is not a risk. Subscribers reporting key compromises to the CA is not a risk since reporting this to the CA enables the CA to take appropriate action.

Question 118

An organization's marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risk assessment. Which of the following should be the MOST important consideration?

- ☒ The information to be exchanged
- ☐ Methods for transferring the information
- ☐ Reputations of the external marketing companies
- ☐ The security of the third-party cloud provider

Licensed to Berend Post berend.post@it-university.nl

Question 119

An IT governance framework provides an organization with:

- ☒ a basis for directing and controlling IT.
- ☐ assurance that there will be IT cost reductions.
- ☐ organizational structures to enlarge the market share through IT.
- ☐ assurance that there are surplus IT investments.

Question 120

Which of the following is MOST important for an IS auditor to consider when determining an appropriate sample size in situations where selecting the entire population is not feasible?

- ☒ Tolerable error
- ☐ Accessibility of the data
- ☐ Data integrity
- ☐ Responsiveness of the auditee

Question 121

Which of the following methods would be MOST effective in verifying that all changes have been authorized?

- ☐ Reconciling problem tickets with authorized change control entries
- ☐ Reconciling reports of changes in production libraries to authorized change log entries
- ☒ Validating authorized change log entries with individual(s) who promoted into production
- ☐ Reconciling reports of changes in development libraries to supporting documentation

Question 122

Well-written risk assessment guidelines for IS auditing should specify which of the following elements at the least (Choose four.)

- ☒ A maximum length for audit cycles.
- ☒ The timing of risk assessments.
- ☒ Documentation requirements.
- ☒ Guidelines for handling special cases.
- ☐ None of the choices.

Explanation:

Explanation:

A well-written risk assessment guidelines should specify a maximum length for audit cycles based on the risk scores and the timing of risk assessments for each department or activity. There should be documentation requirements to support scoring decisions. There should also be guidelines for

Licensed to Berend Post berend.post@it-university.nl

overriding risk assessments in special cases and the circumstances under which they can be overridden.

Question 123

Which of the following would be MOST important to include in a data security policy to adequately manage the privacy of customer information?

- ☒ Information classification criteria
- ☐ Encryption technology
- ☐ Backup strategy
- ☐ Data ownership

Question 124

What method might an IS auditor utilize to test wireless security at branch office locations?

- ☐ War dialing
- ☐ Social engineering
- ☒ War driving
- ☐ Password cracking

Explanation:

Explanation:

War driving is a technique for locating and gaining access to wireless networks by driving or walking with a wireless equipped computer around a building. War dialing is a technique for gaining access to a computer or a network through the dialing of defined blocks of telephone numbers, with the hope of getting an answer from a modem. Social engineering is a technique used to gather information that can assist an attacker in gaining logical or physical access to data or resources. Social engineering exploits human weaknesses. Password crackers are tools used to guess users' passwords by trying combinations and dictionary words.

Question 125

A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- ☐ duplicate check.
- ☐ table lookup.
- ☐ validity check.
- ☒ parity check.

Explanation:

Explanation:

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate

Licensed to Berend Post berend.post@it-university.nl

whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

Question 126

Which of the following would BEST enable alignment of IT with business objectives?

- ☐ Leveraging an IT framework
- ☐ Completing an IT risk assessment
- ☐ Adopting industry best practices
- ☒ Monitoring key performance indicators (KPIs)

Question 127

Which of the following would BEST prevent data from being orphaned?

- ☒ Referential integrity
- ☐ Table partitioning
- ☐ Input validation checks
- ☐ Table indexes

Question 128

During an audit of a telecommunications system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:

- ☒ encryption.
- ☐ callback modems.
- ☐ message authentication.
- ☐ dedicated leased lines.

Explanation:

Explanation:

Encryption of data is the most secure method. The other methods are less secure, with leased lines being possibly the least secure method.

Licensed to Berend Post berend.post@it-university.nl

Question 129

Which of the following should be performed FIRST when preparing to deploy a major upgrade to a critical online application?

- ☐ Update the disaster recovery process.
- ☐ Update the business impact analysis (BIA).
- ☒ Test the rollback process.
- ☐ Review data backup procedures.

Question 130

Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

- ☐ business impact analysis (BIA).
- ☐ threat and risk assessment.
- ☒ business continuity plan (BCP).
- ☐ disaster recovery plan (DRP).

Question 131

Which of the following should an IS auditor recommend as MOST critical to an effective performance improvement process for IT services?

- ☐ Progress on performance goals is regularly reported to the board.
- ☒ The performance goals are aligned with a commonly accepted framework.
- ☐ Root cause analysis of service issues is used to develop performance goals.
- ☐ Management accepts accountability for achieving performance goals.

Question 132

Accountability for the maintenance of appropriate security measures over information assets resides with the:

- ☐ security administrator.
- ☐ systems administrator.
- ☒ data and systems owners.
- ☐ systems operations group.

Explanation:

Explanation:

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

Licensed to Berend Post berend.post@it-university.nl

Question 133

An IS auditor discovered that a firewall has more services than needed. The IS auditor's FIRST recommendation should be to:

- ☐ ensure logging is turned on.
- ☐ deploy a network penetration team.
- ☒ review configurations.
- ☐ eliminate services except for HTTPS.

Question 134

When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

- ☐ Business continuity self-audit
- ☐ Resource recovery analysis
- ☒ Risk assessment
- ☐ Gap analysis

Explanation:

Explanation:

Risk assessment and business impact assessment are tools for understanding business- for- business continuity planning. Business continuity self-audit is a tool for evaluating the adequacy of the BCP, resource recovery analysis is a tool for identifying a business resumption strategy, while the role gap analysis can play in business continuity planning is to identify deficiencies in a plan. Neither of these is used for gaining an understanding of the business.

Question 135

An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- ☐ technical platforms between the two companies are interoperable.
- ☒ parent bank is authorized to serve as a service provider.
- ☐ security features are in place to segregate subsidiary trades.
- ☐ subsidiary can join as a co-owner of this payment system.

Explanation:

Explanation:

Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as banking. Unless granted to serve as a service provider, it may not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security

Licensed to Berend Post berend.post@it-university.nl

aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider. The ownership of the payment system is not as important as the legal authorization to operate the system.

Question 136

Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

- ☒ existence of a set of functions and their specified properties.
- ☐ ability of the software to be transferred from one environment to another.
- ☐ capability of software to maintain its level of performance under stated conditions.
- ☐ relationship between the performance of the software and the amount of resources used.

Explanation:

Explanation:

Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability; choice C refers to reliability and choice D refers to efficiency.

Question 137

Your final audit report should be issued:

- ☒ after an agreement on the observations is reached.
- ☐ before an agreement on the observations is reached.
- ☐ if an agreement on the observations cannot reached.
- ☐ without mentioning the observations.
- ☐ None of the choices.

Explanation:

Explanation:

Reporting can take the forms of verbal presentation, an issue paper or a written audit report summarizing observations and management's responses. After agreement is reached on the observations, a final report can be issued.

Licensed to Berend Post berend.post@it-university.nl

Question 138

To develop meaningful recommendations for findings, which of the following is MOST important for an IS auditor to determine and understand?

- ☐ Criteria
- ☐ Responsible party
- ☒ Impact
- ☐ Root cause

Question 139

An IS auditor considering the risks associated with spooling sensitive reports for off-line printing will be the MOST concerned that:

- ☐ data can easily be read by operators
- ☐ data can more easily be amended by unauthorized persons
- ☒ unauthorized copies of reports can be printed
- ☐ output will be lost if the system should fail

Question 140

A substantive test to verify that tape library inventory records are accurate is:

- ☐ determining whether bar code readers are installed.
- ☐ determining whether the movement of tapes is authorized.
- ☒ conducting a physical count of the tape inventory.
- ☐ checking if receipts and issues of tapes are accurately recorded.

Explanation:

Explanation:

A substantive test includes gathering evidence to evaluate the integrity of individual transactions, data or other information. Conducting a physical count of the tape inventory is a substantive test. Choices A, B and D are compliance tests.

Question 141

Which of the following is an example of audit risk?

- ☐ Audit work may be lost due to a malware attack.
- ☐ Management may disagree with audit conclusions.
- ☒ Sampling methods may not detect a material error.
- ☐ Newer auditors may require additional supervision and training.

Licensed to Berend Post berend.post@it-university.nl

Question 142

A programmer has made unauthorized changes to key fields in a payroll system report. Which of the following control weaknesses would have contributed MOST to this problem?

- ☐ The user requirements were not documented.
- ☐ Payroll files were not under the control of a librarian.
- ☐ The programmer did not involve the user in testing.
- ☒ The programmer has access to the production programs.

Question 143

When evaluating the recent implementation of an intrusion detection system (IDS), an IS auditor should be MOST concerned with inappropriate:

- ☐ encryption.
- ☐ training.
- ☒ tuning.
- ☐ patching.

Question 144

An IS auditor has been asked to review a recently implemented quality management system (QMS). Which of the following should be the auditor's PRIMARY focus?

- ☐ Training materials prepared for coaching employees
- ☒ Processes to measure the performance of business critical transactions
- ☐ Documentation standard of the implemented QMS system
- ☐ Stability of the implemented QMS system over a period of time

Question 145

Which of the following could an IS auditor recommend to improve the estimated resources required in system development?

- ☐ Business areas involvement
- ☐ Prototyping
- ☒ Function point analysis
- ☐ CASE tools

Licensed to Berend Post berend.post@it-university.nl

Question 146

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

- ☐ manual processing capabilities and the test location.
- ☒ the importance of the function to be tested and the cost of testing.
- ☐ the experience level of personnel and the function location.
- ☐ prior testing results and the degree of detail of the business continuity plan.

Question 147

Which of the following audit include specific tests of control to demonstrate adherence to specific regulatory or industry standard?

- ☒ Compliance Audit
- ☐ Financial Audit
- ☐ Operational Audit
- ☐ Forensic audit

Explanation:

Explanation:

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

For your exam you should know below information about different types of audit:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization’s accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and

Licensed to Berend Post berend.post@it-university.nl

risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

Licensed to Berend Post berend.post@it-university.nl

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

Financial Audit- A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework.

Operational Audit - Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. [1] Operational audit is a more comprehensive form of an Internal audit.

Forensic Audit - Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 47

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

Question 148

Which of the following should be an IS auditor's FIRST activity when planning an audit?

- ☒ Gain an understanding of the area to be audited.
- ☐ Document specific questions in the audit program.
- ☐ Create a list of key controls to be reviewed.
- ☐ Identify proper resources for audit activities.

Licensed to Berend Post berend.post@it-university.nl

Question 149

Electrical surge protectors BEST protect from the impact of:

- ☐ electromagnetic interference.
- ☐ power outages.
- ☒ sags and spikes
- ☐ reduced voltage.

Question 150

The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

- ☐ rules.
- ☒ decision trees.
- ☐ semantic nets.
- ☐ dataflow diagrams.

Explanation:

Explanation:

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

Question 151

An audit charter should:

- ☐ be dynamic and change often to coincide with the changing nature of technology and the audit profession.
- ☐ clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
- ☐ document the audit procedures designed to achieve the planned audit objectives.
- ☒ outline the overall authority, scope and responsibilities of the audit function.

Explanation:

Explanation:

An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

Licensed to Berend Post berend.post@it-university.nl

Question 152

Which of the following is the process of feeding test data into two systems – the modified system and alternative system and comparing the result?

- ☒ Parallel Test
- ☐ Black box testing
- ☐ Regression Testing
- ☐ Pilot Testing

Explanation:

Parallel testing is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Licensed to Berend Post berend.post@it-university.nl

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:

Regression Testing -The process of returning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 167

Licensed to Berend Post berend.post@it-university.nl

Question 153

An audit committee is reviewing an annual IT risk assessment. Which of the following is the BEST justification for the audits selected?

- ☐ Likelihood of an IT process failure
- ☐ Key IT general process controls
- ☐ Applications impacted
- ☒ Underlying business risks

Question 154

The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

- ☒ integrity.
- ☐ authenticity.
- ☐ authorization.
- ☐ nonrepudiation.

Explanation:

Explanation:

A checksum calculated on an amount field and included in the EDI communication can be used to identify unauthorized modifications. Authenticity and authorization cannot be established by a checksum alone and need other controls. Nonrepudiation can be ensured by using digital signatures.

Question 155

Which of the following transmission media would NOT be affected by cross talk or interference?

- ☐ Copper cable
- ☐ Radio System
- ☐ Satellite radio link
- ☒ Fiber optic cables

Explanation:

Only fiber optic cables are not affected by crosstalk or interference.

For your exam you should know the information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Licensed to Berend Post berend.post@it-university.nl

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video

Coaxial Cable

Licensed to Berend Post berend.post@it-university.nl

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System

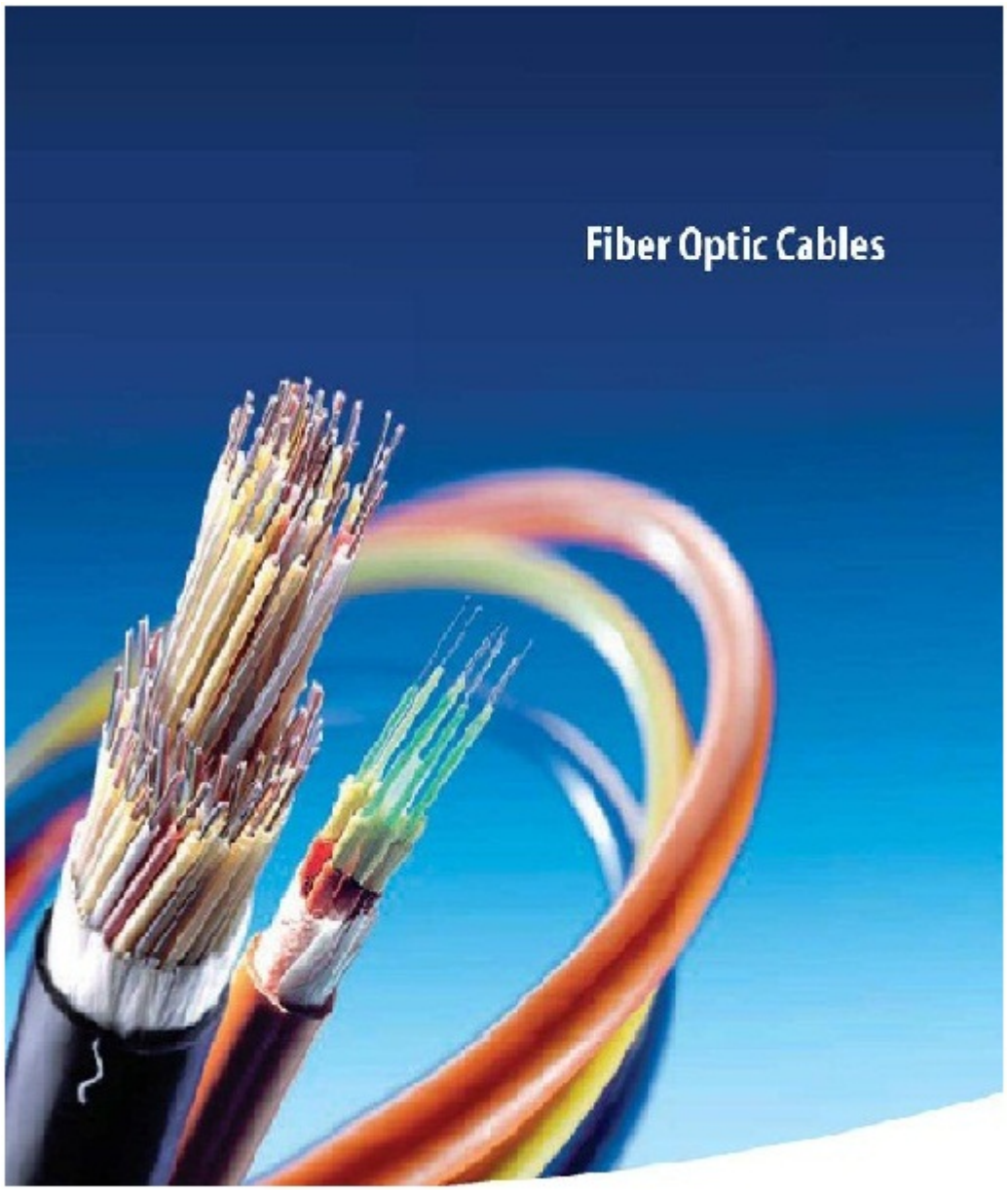
Radio systems are used for short distance, cheap and easy to tap.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

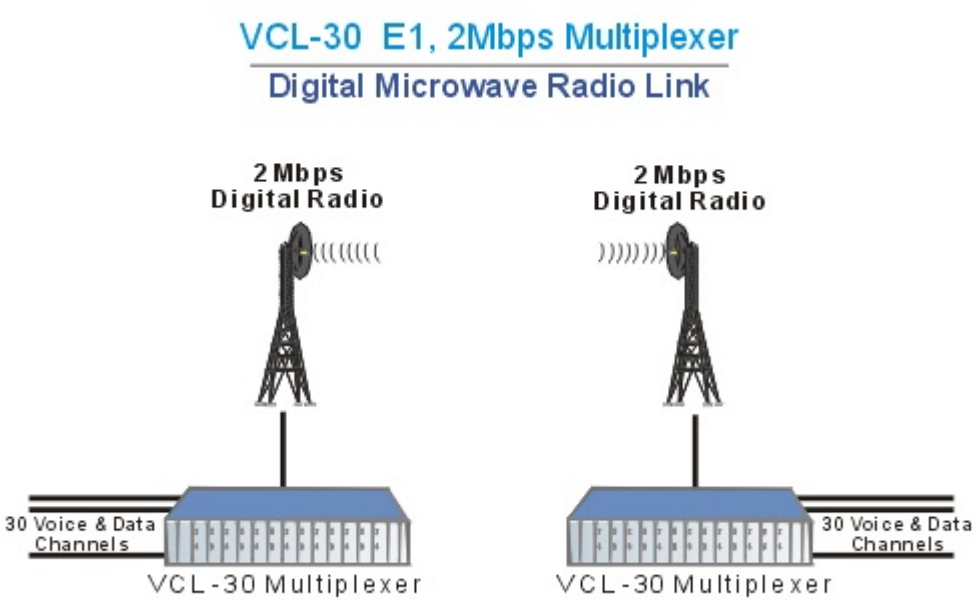
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Licensed to Berend Post berend.post@it-university.nl

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to tap.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Licensed to Berend Post berend.post@it-university.nl

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265 &

Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

Question 156

Which of the following is a control over component communication failure/errors?

- ☐ Restricting operator access and maintaining audit trails
- ☐ Monitoring and reviewing system engineering activity
- ☒ Providing network redundancy
- ☐ Establishing physical barriers to the data transmitted over the network

Explanation:

Explanation:

Redundancy by building some form of duplication into the network components, such as a link, router or switch to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echochecks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls.

Question 157

After initial investigation, an IS auditor has reasons to believe that fraud may be present.
The IS auditor should:

- ☒ expand activities to determine whether an investigation is warranted
- ☐ report the matter to the audit committee.
- ☐ report the possibility of fraud to top management and ask how they would like to be proceed.
- ☐ consult with external legal counsel to determine the course of action to be taken.

Explanation:

Explanation:

An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

Licensed to Berend Post berend.post@it-university.nl

Question 158

A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

- ☒ Whether key controls are in place to protect assets and information resources
- ☐ If the system addresses corporate customer requirements
- ☐ Whether the system can meet the performance goals (time and resources)
- ☐ Whether owners have been identified who will be responsible for the process

Explanation:

Explanation:

The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the business process reengineering (BPR) process should achieve, but they are not the auditor's primary concern.

Question 159

Which of the following statements pertaining to IPSec is incorrect?

- ☒ A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
- ☐ Integrity and authentication for IP datagrams are provided by AH.
- ☐ ESP provides for integrity, authentication and encryption to IP datagram's.
- ☐ In transport mode, ESP only encrypts the data payload of each packet.

Explanation:

This is incorrect, there would be a pair of Security Association (SA) needed for bi directional communication and NOT only one SA. The sender and the receiver would both negotiate an SA for inbound and outbound connections.

The two main concepts of IPSec are Security Associations (SA) and tunneling. A Security Association (SA) is a simplex logical connection between two IPSec systems. For bi-directional communication to be established between two IPSec systems, two separate Security Associations, one in each direction, must be defined.

The security protocols can either be AH or ESP.

The explanations below are a bit more thorough than what you need to know for the exam. However, they always say a picture is worth one thousand words, I think it is very true when it comes to explaining IPSEC and it's inner working. I have found a great article from CISCO PRESS and DLINK covering this subject, see references below.

Licensed to Berend Post berend.post@it-university.nl

Tunnel and Transport Modes

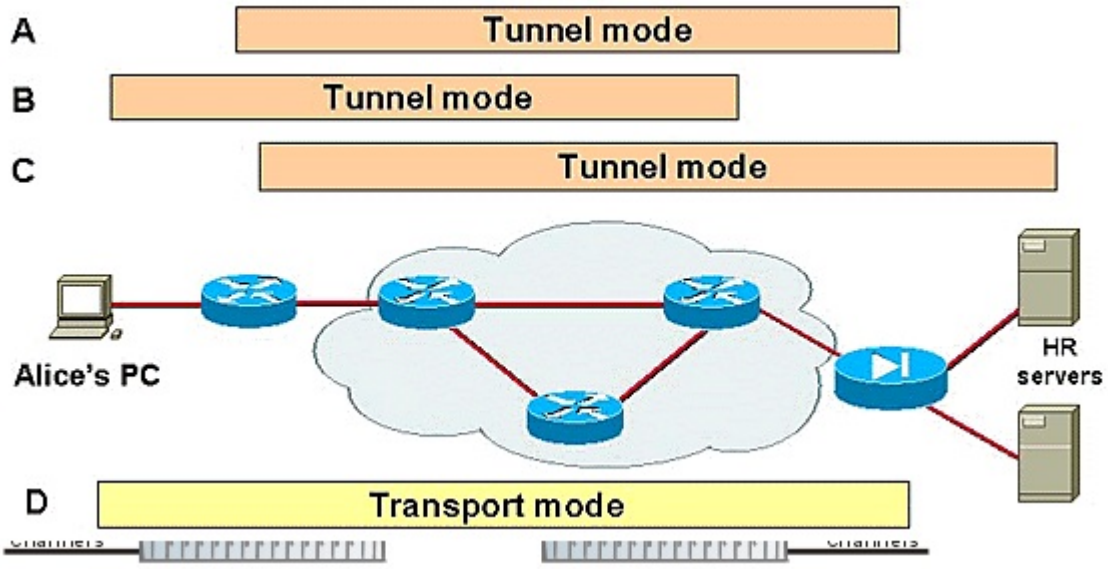
IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

Transport mode is used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.

As you can see in the Figure 1 graphic below, basically transport mode should be used for end-to-end sessions and tunnel mode should be used for everything else.

FIGURE: 1



IPSEC Transport Mode versus Tunnel Mode

Tunnel and transport modes in IPSec.

Figure 1 above displays some examples of when to use tunnel versus transport mode:

Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such as Alice's PC and the HR servers in Figure 1. In example A, Alice connects to the HR servers securely through the IPSec tunnel set up between the gateways.

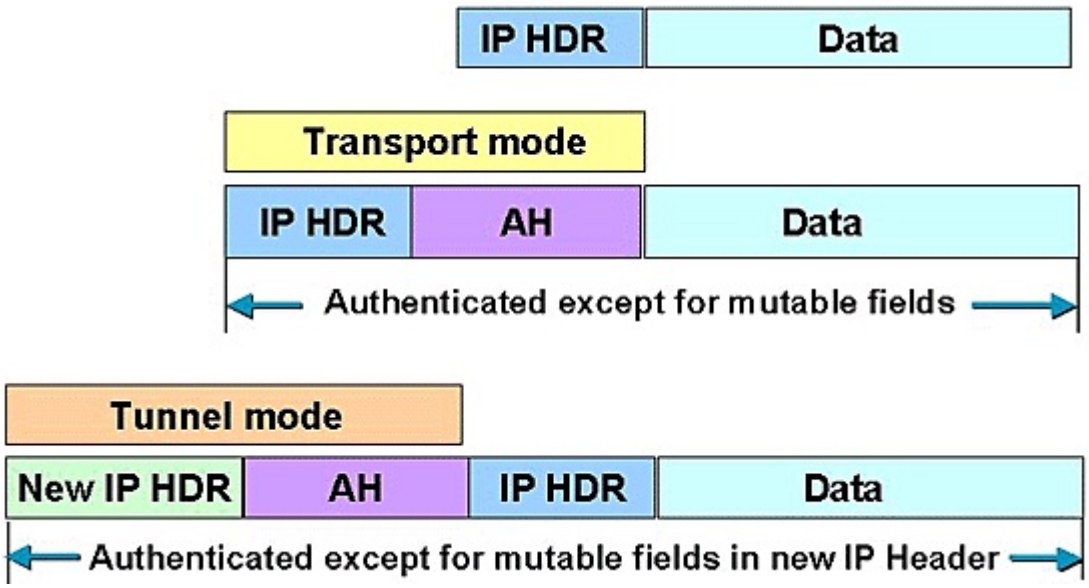
Licensed to Berend Post berend.post@it-university.nl

Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B.

In example C, tunnel mode is used to set up an IPSec tunnel between the Cisco router and a server running IPSec software. Note that Cisco IOS software and the PIX Firewall sets tunnel mode as the default IPSec mode.

Transport mode is used between end-stations supporting IPSec, or between an end-station and a gateway, if the gateway is being treated as a host. In example D, transport mode is used to set up an encrypted Telnet session from Alice's PC running Cisco Secure VPN Client software to terminate at the PIX Firewall, enabling Alice to remotely configure the PIX Firewall securely.

FIGURE: 2



IPSEC AH Tunnel and Transport mode

AH Tunnel Versus Transport Mode

Figure 2 above, shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that don't change in transport. The header goes after the IP header and before the ESP header, if present, and other higher-layer protocols.

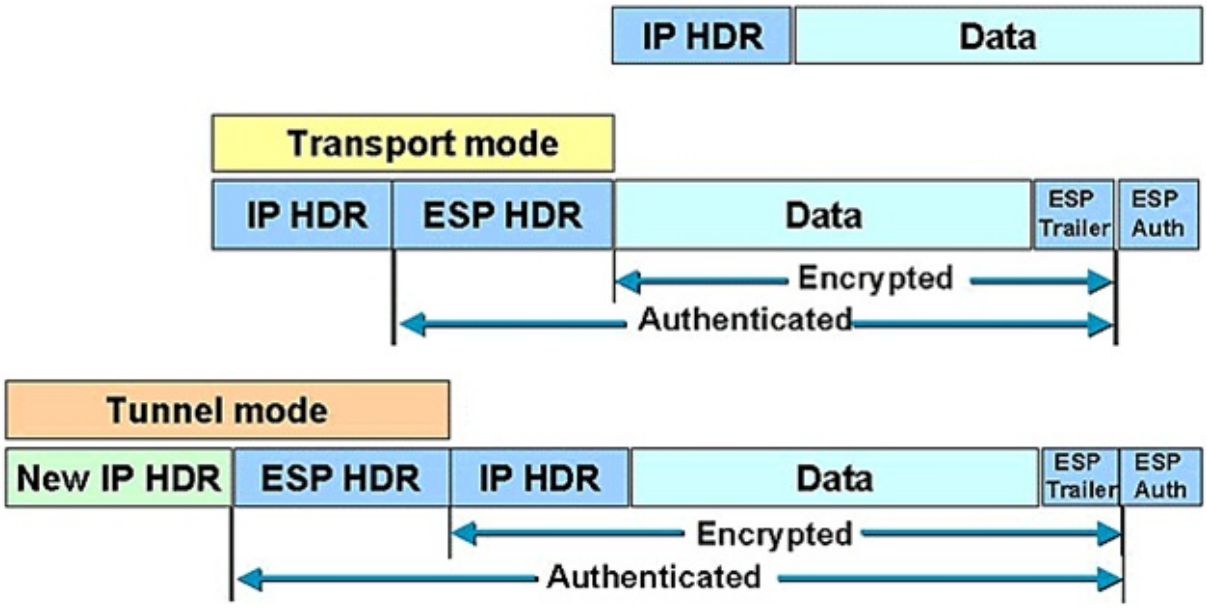
As you can see in Figure 2 above, In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.

Licensed to Berend Post berend.post@it-university.nl

AH is incompatible with Network Address Translation (NAT) because NAT changes the source IP address, which breaks the AH header and causes the packets to be rejected by the IPSec peer.

FIGURE: 3

IPSEC ESP Tunnel versus Transport modes



ESP Tunnel Versus Transport Mode

Figure 3 above shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP doesn't authenticate the IP header itself.

NOTE: Higher-layer information is not available because it's part of the encrypted payload.

When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.

When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Prior to decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.

Licensed to Berend Post berend.post@it-university.nl

ESP can also provide packet authentication with an optional field for authentication. Cisco IOS software and the PIX Firewall refer to this service as ESP hashed message authentication code (HMAC). Authentication is calculated after the encryption is done. The current IPSec standard specifies which hashing algorithms have to be supported as the mandatory HMAC algorithms.

The main difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP doesn't protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode).

The following were incorrect answers for this question:

Integrity and authentication for IP datagrams are provided by AH This is correct, AH provides integrity and authentication and ESP provides integrity, authentication and encryption.

ESP provides for integrity, authentication and encryption to IP datagram's. ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

In transport mode, ESP only encrypts the data payload of each packet. ESP can be operated in either tunnel mode (where the original packet is encapsulated into a new one) or transport mode (where only the data payload of each packet is encrypted, leaving the header untouched).

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6986-6989). Acerbic Publications. Kindle Edition.

and

http://www.ciscopress.com/articles/article.asp?p=25477

and

http://documentation.netgear.com/reference/sve/vpn/VPNBasics-3-05.html

Licensed to Berend Post berend.post@it-university.nl

Question 160

Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

- ☐ Exposures
- ☒ Threats
- ☐ Hazards
- ☐ Insufficient controls

Explanation:

Explanation:

Threats exploit vulnerabilities to cause loss or damage to the organization and its assets.

Question 161

Which of the following is an advantage of the top-down approach to software testing?

- ☒ Interface errors are identified early
- ☐ Testing can be started before all programs are complete
- ☐ it is more effective than other testing approaches
- ☐ Errors in critical modules are detected sooner

Explanation:

Explanation:

The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner. The most effective testing approach is dependent on the environment being tested. Choices B and D are advantages of the bottom-up approach to system testing.

Question 162

An organization with a maturing incident response program conducts post-incident reviews for all major information security incidents. The PRIMARY goal of these reviews should be to:

- ☒ identify security program gaps or systemic weaknesses that need correction.
- ☐ prepare properly vetted notifications regarding the incidents to external parties.
- ☐ identify who should be held accountable for the security incidents.
- ☐ document and report the root cause of the incidents for senior management.

Licensed to Berend Post berend.post@it-university.nl

Question 163

Which of the following statement correctly describes the difference between symmetric key encryption and asymmetric key encryption?

☐ In symmetric key encryption the same key is used for encryption and decryption where as asymmetric key uses private key for encryption and decryption

☐ In symmetric key encryption the public key is used for encryption and the symmetric key for decryption. Where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption

☒ In symmetric key encryption the same key is used for encryption and decryption where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption.

☐ Both uses private key for encryption and the decryption process can be done using public key

Explanation:

There are two basic techniques for encrypting information: symmetric encryption (also called secret key encryption) and asymmetric encryption (also called public key encryption.)

Symmetric Encryption

Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Few examples of symmetric key algorithms are DES, AES, Blowfish, etc

Asymmetric Encryption

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is the usage of asymmetric encryption, in which there are two related keys, usually called a key pair. The public key is made freely available to anyone who might want to send you a message. The second key, called the private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted using the public key can only be decrypted by the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public).A problem with asymmetric encryption, however, is that it is slower than

Licensed to Berend Post berend.post@it-university.nl

symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

Few examples of asymmetric key algorithms are RSA, Elliptic key Cryptography (ECC), El Gamal, Differ-Hellman, etc

The following were incorrect answers:

The other options don't describe correctly the difference between symmetric key and asymmetric key encryption.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348 and 349

http://support.microsoft.com/kb/246071

Question 164

Which of the following would be the BEST way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)?

- ☐ Perform industry research annually and document the overall ranking of the IPS.
- ☐ Perform a penetration test to demonstrate the ability to protect.
- ☒ Establish and present appropriate metrics that track performance.
- ☐ Provide yearly competitive pricing to illustrate the value of the IPS.

Question 165

Which of the following is the PRIMARY concern if a business continuity plan (BCP) is not based on a business impact analysis (BIA)?

- ☐ The critical systems were not identified, but all systems are covered in the BCP.
- ☐ The knowledge of key people within the organization was not considered in the BCP.
- ☐ The strategy of the BCP does not reflect estimated potential losses.
- ☒ Management was not involved in the early stages of the BCP.

Licensed to Berend Post berend.post@it-university.nl

Question 166

An IS auditor is assigned to review the development of a specific application. Which of the following would be the MOST significant step following the feasibility study?

- ☐ Attend project progress meetings to monitor timely implementation of the application.
- ☐ Assist users in the design of proper acceptance-testing procedures.
- ☒ Follow up with project sponsor for project's budgets and actual costs.
- ☐ Review functional design to determine that appropriate controls are planned.

Question 167

What are intrusion-detection systems (IDS) primarily used for?

- ☐ To identify AND prevent intrusion attempts to a network
- ☐ To prevent intrusion attempts to a network
- ☐ Forensic incident response
- ☒ To identify intrusion attempts to a network

Explanation:

Explanation:

Intrusion-detection systems (IDS) are used to identify intrusion attempts on a network.

Question 168

When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

- ☐ The potential for unauthorized deletion of report copies
- ☐ The potential for unauthorized modification of report copies
- ☒ The potential for unauthorized printing of report copies
- ☐ The potential for unauthorized editing of report copies

Explanation:

Explanation:

When reviewing print systems spooling, an IS auditor is most concerned with the potential for unauthorized printing of report copies.

Licensed to Berend Post berend.post@it-university.nl

Question 169

Which of the following is the MOST important role of the information security manager when the organization is in the process of adopting emerging technologies?

- ☒ Understanding the impact on existing resources
- ☐ Assessing how peer organizations using the same technologies have been impacted
- ☐ Developing training for end users to familiarize them with the new technology
- ☐ Reviewing vendor documentation and service levels agreements

Question 170

Which of the following refers to an important procedure when evaluating database security?

- ☒ performing vulnerability assessments against the database.
- ☐ performing data check against the database.
- ☐ performing dictionary check against the database.
- ☐ performing capacity check against the database system.
- ☐ None of the choices.

Explanation:

Explanation:

Databases provide many layers and types of security, including Access control, Auditing, Authentication, Encryption and Integrity controls. An important procedure when evaluating database security is performing vulnerability assessments against the database. Database administrators or Information security administrators run vulnerability scans on databases to discover misconfiguration of controls within the layers mentioned above along with known vulnerabilities within the database software.

Question 171

Which of the following is MOST important for an organization to complete when planning a new marketing platform that targets advertising based on customer behavior?

- ☒ Data privacy impact assessment
- ☐ Data quality assessment
- ☐ Cross-border data transfer assessment
- ☐ Security vulnerability assessment

Licensed to Berend Post berend.post@it-university.nl

Question 172

What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

- ☐ A combination of public-key cryptography and digital certificates and two-factor authentication
- ☐ A combination of public-key cryptography and two-factor authentication
- ☒ A combination of public-key cryptography and digital certificates
- ☐ A combination of digital certificates and two-factor authentication

Explanation:

Explanation:

PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

Question 173

After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

- ☐ Differential reporting
- ☐ False-positive reporting
- ☒ False-negative reporting
- ☐ Less-detail reporting

Explanation:

Explanation:

False-negative reporting on weaknesses means the control weaknesses in the network are not identified and therefore may not be addressed, leaving the network vulnerable to attack. False-positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

Question 174

Which of the following is the MOST reliable form of single factor personal identification?

- ☐ Smart card
- ☐ Password
- ☐ Photo identification
- ☒ iris scan

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Since no two irises are alike, identification and verification can be done with confidence. There is no guarantee that a smart card is being used by the correct person since it can be shared, stolen or lost and found. Passwords can be shared and, if written down, carry the risk of discovery.

Photo IDs can be forged or falsified.

Question 175

In planning an audit, the MOST critical step is the identification of the:

- ☒ areas of high risk.
- ☐ skill sets of the audit staff.
- ☐ test steps in the audit.
- ☐ time allotted for the audit.

Explanation:

Explanation:

When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Test steps for the audit are not as critical as identifying the areas of risk, and the time allotted for an audit is determined by the areas to be audited, which are primarily selected based on the identification of risks.

Question 176

While auditing an IT department's cloud service provider, the IS auditor found that privileged access monitoring is not being performed as required by the contract. The provider disagrees with this issue and noted that compensating controls are in place. The IS auditor's NEXT course of action should be to:

- ☒ test compensating controls as part of the audit.
- ☐ define a remediation plan.
- ☐ review privileged access logs.
- ☐ recommend revising the service level agreement (SLA).

Question 177

Ensuring that security and control policies support business and IT objectives is a primary objective of:

- ☒ An IT security policies audit
- ☐ A processing audit
- ☐ A software audit
- ☐ A vulnerability assessment

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Ensuring that security and control policies support business and IT objectives is a primary objective of an IT security policies audit.

Question 178

An IS auditor auditing the effectiveness of utilizing a hot site will MOST likely:

- ☐ review reciprocal agreements.
- ☐ review logical access controls.
- ☐ evaluate physical access controls.
- ☒ analyze system restoration procedures.

Question 179

An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

- ☐ IDS sensors are placed outside of the firewall.
- ☐ a behavior-based IDS is causing many false alarms.
- ☐ a signature-based IDS is weak against new types of attacks.
- ☒ the IDS is used to detect encrypted traffic.

Explanation:

Explanation:

An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks.

These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature- based IDS, because it can only recognize attacks that have been previously identified.

Question 180

When determining whether a project in the design phase will meet organizational objectives, what is BEST to compare against the business case?

- ☐ Project plan
- ☒ Requirements analysis
- ☐ Implementation plan
- ☐ Project budget provisions

Licensed to Berend Post berend.post@it-university.nl

Question 181

Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?

- ☒ exploit
- ☐ patch
- ☐ quick fix
- ☐ service pack
- ☐ malware
- ☐ None of the choices.

Explanation:

Explanation:

"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

Question 182

Which of the following BEST demonstrates to an IS auditor that an organization has implemented effective risk management processes?

- ☐ Critical business assets have additional controls.
- ☒ The risk register is reviewed periodically.
- ☐ A business impact analysis (BIA) has been completed.
- ☐ The inventory of IT assets includes asset classification.

Question 183

An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resources to support clients. The BEST approach to obtain the support of business unit management would be to:

- ☐ elaborate on the positive impact to information security.
- ☐ present industry benchmarking results to business units.
- ☒ discuss the risk and impact of security incidents if not implemented.
- ☐ present an analysis of the cost and benefit of the changes.

Licensed to Berend Post berend.post@it-university.nl

Question 184

The PRIMARY objective of a logical access control review is to:

- ☐ review access controls provided through software.
- ☒ ensure access is granted per the organization's authorities.
- ☐ walk through and assess the access provided in the IT environment.
- ☐ provide assurance that computer hardware is adequately protected against abuse.

Explanation:

Explanation:

The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

Question 185

Which of the following is the BEST way for management to ensure the effectiveness of the cybersecurity incident response process?

- ☐ Periodic update of incident response process documentation
- ☐ Periodic reporting of cybersecurity incidents to key stakeholders
- ☒ Periodic tabletop exercises involving key stakeholders
- ☐ Periodic cybersecurity training for staff involved in incident response

Question 186

Which of the following types of firewalls would BEST protect a network from an internet attack?

- ☒ Screened subnet firewall
- ☐ Application filtering gateway
- ☐ Packet filtering router
- ☐ Circuit-level gateway

Explanation:

Explanation:

A screened subnet firewall would provide the best protection. The screening router can be a commercial router or a node with routing capabilities and the ability to allow or avoid traffic between nets or nodes based on addresses, ports, protocols, interfaces, etc. Application-level gateways are mediators between two entities that want to communicate, also known as proxy gateways. The application level (proxy) works at the application level, not just at a package level. The screening controls at the package level, addresses and ports, but does not see the contents of the package. A packet filtering router examines the header of every packet or data traveling between the internet and the corporate network.

Licensed to Berend Post berend.post@it-university.nl

Question 187

A data leakage prevention (DLP) solution has identified that several employees are sending confidential company data to their personal email addresses in violation of company policy. The information security manager should FIRST:

- ☒ initiate an investigation to determine the full extent of noncompliance
- ☐ notify senior management that employees are breaching policy
- ☐ limit access to the Internet for employees involved
- ☐ contact the employees involved to retake security awareness training

Question 188

When implementing an upgraded ERP system, which of the following is the MOST important consideration for a go-live decision?

- ☐ Test cases
- ☐ Rollback strategy
- ☒ Business case
- ☐ Post-implementation review objectives

Question 189

A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

- ☒ analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
- ☐ WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.
- ☐ the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
- ☐ users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

Explanation:

Explanation:

The peak at 96 percent could be the result of a one-off incident, e.g., a user downloading a large amount of data; therefore, analysis to establish whether this is a regular pattern and what causes this behavior should be carried out before expenditure on a larger line capacity is recommended. Since the link provides for a standby database, a short loss of this service should be acceptable. If the peak is established to be a regular occurrence without any other opportunities for mitigation (usage of bandwidth reservation protocol, or other types of prioritizing network traffic), the line should be replaced as there is the risk of loss of service as the traffic approaches 100 percent. If, however, the peak is a one-off or can be put in other time frames, then user education may be an option.

Licensed to Berend Post berend.post@it-university.nl

Question 190

Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

- ☐ System analysis
- ☒ Authorization of access to data
- ☐ Application programming
- ☐ Data administration

Explanation:

Explanation:

The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

Question 191

A company converted its payroll system from an external service to an internal package. Payroll processing in April was run in parallel. To validate the completeness of data after the conversion, which of the following comparisons from the old to the new system would be MOST effective?

- ☐ Turnaround time for payroll processing
- ☐ Employee counts and year-to-date payroll totals
- ☒ Master file employee data to payroll journals
- ☐ Cut-off dates and overwrites for a sample of employees

Question 192

When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

- ☒ Wiring and schematic diagram
- ☐ Users' lists and responsibilities
- ☐ Application lists and their details
- ☐ Backup and recovery procedures

Explanation:

Explanation:

The wiring and schematic diagram of the network is necessary to carry out a network audit. A network audit may not be feasible if a network wiring and schematic diagram is not available. All other documents are important but not necessary.

Licensed to Berend Post berend.post@it-university.nl

Question 193

When conducting a follow-up audit on an organization's firewall configuration, the IS auditor discovered that the firewall had been integrated into a new system that provides both firewall and intrusion detection capabilities. The IS auditor should:

- ☐ consider the follow-up audit unnecessary since the firewall is no longer being used.
- ☒ assess whether the integrated system addresses the identified risk.
- ☐ review the compatibility of the new system with existing network controls.
- ☐ evaluate whether current staff is able to support the new system.

Question 194

Which of the following is the MOST important element when developing an information security strategy?

- ☐ Identifying applicable laws and regulations
- ☐ Identifying information assets
- ☐ Determining the risk management methodology
- ☒ Aligning security activities with organizational goals

Question 195

Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

- ☐ Bridge
- ☐ Repeater
- ☐ Router
- ☒ Gateway

Explanation:

A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

Important Note:

For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.

The second thing you must remembers is the fact that a gateway act as a translation device.

It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know the information below:

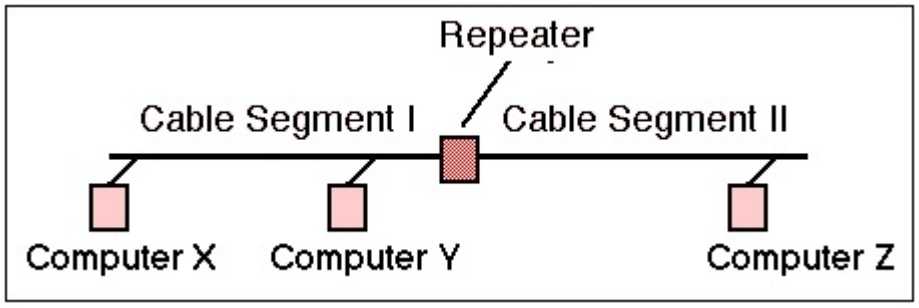
Repeaters

A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.

A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

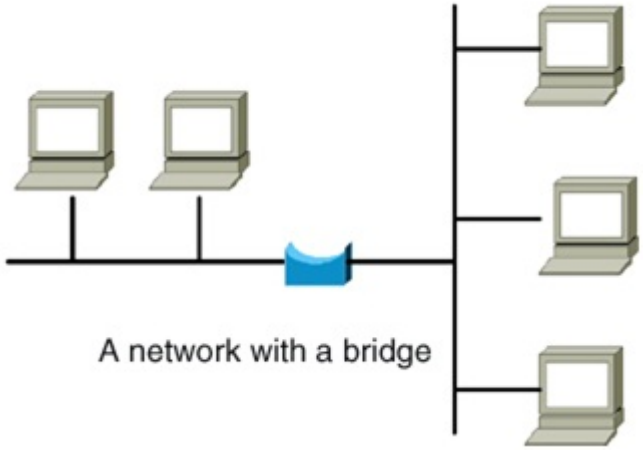


Bridges

A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

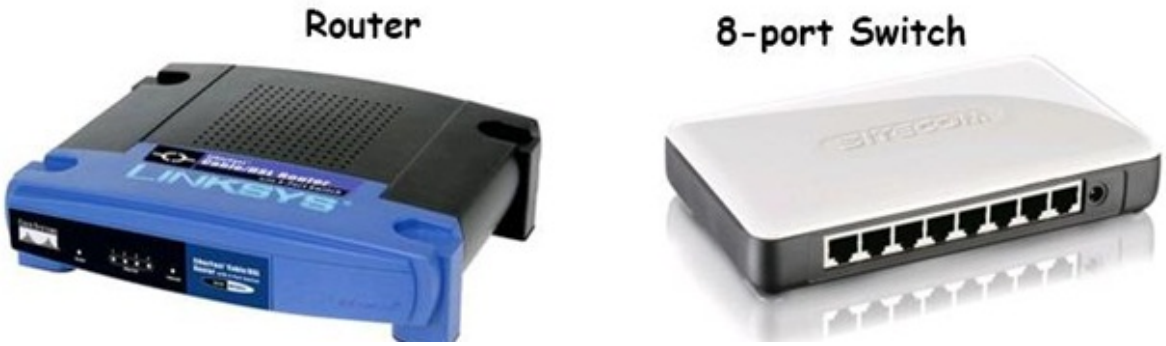
Licensed to Berend Post berend.post@it-university.nl



Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch



Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

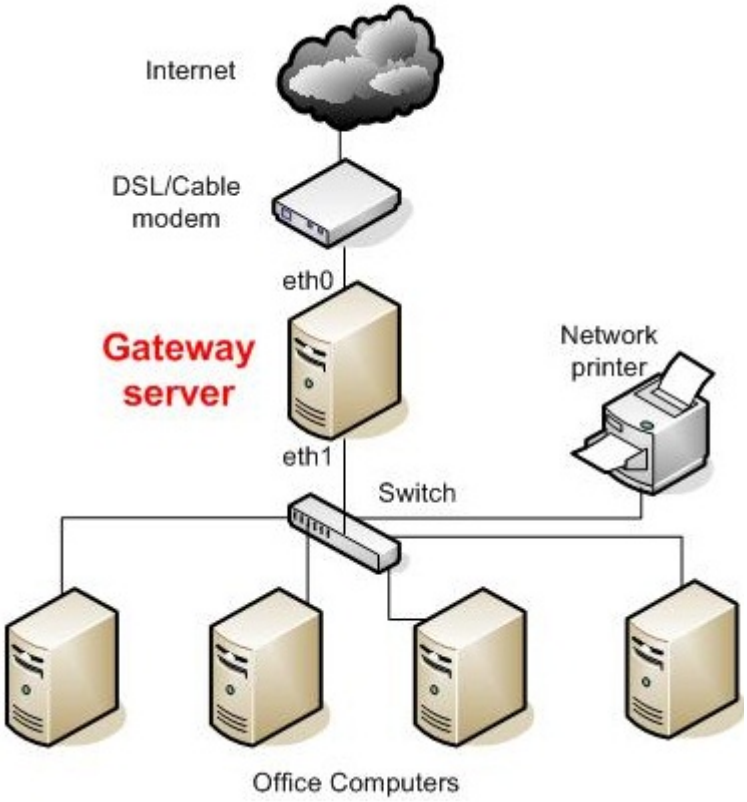
Gateways

Licensed to Berend Post berend.post@it-university.nl

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol

packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server



The following answers are incorrect:

Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC

Licensed to Berend Post berend.post@it-university.nl

address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 263

Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

Question 196

Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

- ☒ Virtual private network
- ☐ Dedicated line
- ☐ Leased line
- ☐ integrated services digital network

Explanation:

Explanation:

The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small- to medium-sized organizations.

Question 197

Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

- ☐ Security awareness
- ☐ Reading the security policy
- ☐ Security committee
- ☒ Logical access controls

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent the unauthorized access of information. A security committee (choice C) is key to the protection of information assets, but would address security issues within a broader perspective.

Question 198

An IS auditor should expect the responsibility for authorizing access rights to production data and systems to be entrusted to the:

- ☐ process owners.
- ☐ system administrators.
- ☐ security administrator.
- ☒ data owners.

Explanation:

Explanation:

Data owners are primarily responsible for safeguarding the data and authorizing access to production data on a need-to-know basis.

Question 199

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- ☐ Wet-pipe sprinkler system
- ☐ Dry-pipe sprinkler system
- ☒ FM-200system
- ☐ Carbon dioxide-based fire extinguishers

Explanation:

Explanation:

FM-200 is safer to use than carbon dioxide. It is considered a clean agent for use in gaseous fire suppression applications. A water-based fire extinguisher is suitable when sensitive computer equipment could be damaged before the fire department personnel arrive at the site. Manual firefighting (fire extinguishers) may not provide fast enough protection for sensitive equipment (e.g., network servers).

Licensed to Berend Post berend.post@it-university.nl

Question 200

What should be the MAIN goal of an organization's incident response plan?

- ☐ Keep stakeholders notified of incident status.
- ☐ Enable appropriate response according to criticality.
- ☐ Correlate incidents from different systems.
- ☒ Identify the root cause of the incident.

Question 201

Which of the following layer in an enterprise data flow architecture derives enterprise information from operational data, external data and nonoperational data?

- ☐ Data preparation layer
- ☒ Data source layer
- ☐ Data mart layer
- ☐ Data access layer

Explanation:

Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Licensed to Berend Post berend.post@it-university.nl

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Licensed to Berend Post berend.post@it-university.nl

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Licensed to Berend Post berend.post@it-university.nl

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Data mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 202

An IS auditor's PRIMARY concern about a business partner agreement for the exchange of electronic information should be to determine whether there is:

- ☐ a clause that addresses the audit of shared systems.
- ☐ evidence of review and approval by each partner's legal department.
- ☒ an information classification framework.
- ☐ appropriate control and responsibility defined for each partner.

Explanation:

Explanation:

The overall purpose of using a formal information classification scheme is to ensure proper handling based on the information content and context. Context refers to the usage of information.

Two major risks are present in the absence of an information classification scheme. The first major risk is that information will be mishandled. The second major risk is that without an information

 Licensed to Berend Post berend.post@it-university.nl

classification scheme, all of the organization's data may be subject to scrutiny during legal proceedings. The information classification scheme safeguards knowledge. Failure to implement a records and data classification scheme leads to disaster

Question 203

Wi-Fi Protected Access implements the majority of which IEEE standard?

- ☒ 802.11i
- ☐ 802.11g
- ☐ 802.11x
- ☐ 802.11v
- ☐ None of the choices.

Explanation:

Explanation:

Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

Question 204

Identify the INCORRECT statement from below mentioned testing types

- ☒ Recovery Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems
- ☐ Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour
- ☐ Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process
- ☐ Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

Explanation:

The word INCORRECT is the keyword used in this question. You need to find out the incorrect option specified above. The term recovery testing is incorrectly defined in the above options. The correct description of recovery testing is: Recovery Testing – Checking the system's ability to recover after a software or hardware failure

For CISA exam you should know below types of testing:

Licensed to Berend Post berend.post@it-university.nl

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the system's ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.

QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the

Licensed to Berend Post berend.post@it-university.nl

application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include:

Definition of test strategies and procedure.

Design of test cases and scenarios

Execution of the tests.

Utilization of the result to verify system readiness.

Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:

The other options presented contains valid definitions.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 166

Question 205

The MOST important reason to use a centralized mechanism to identify information security incidents is to:

- ☐ prevent unauthorized changes to networks.
- ☐ comply with corporate policies.
- ☐ detect potential fraud.
- ☒ detect threats across environments.

Licensed to Berend Post berend.post@it-university.nl

Question 206

An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

- ☒ Stricter controls should be implemented by both the organization and the cleaning agency.
- ☐ No action is required since such incidents have not occurred in the past.
- ☐ A clear desk policy should be implemented and strictly enforced in the organization.
- ☐ A sound backup policy for all important office documents should be implemented.

Explanation:

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact.

Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

Question 207

During a software acquisition review, an IS auditor should recommend that there be a software escrow agreement when:

- ☐ the estimated life for the product is less than 3 years.
- ☒ the deliverables do not include the source code.
- ☐ the product is new in the market.
- ☐ there is no service level agreement (SLA).

Question 208

What often results in project scope creep when functional requirements are not defined as well as they could be?

- ☒ Inadequate software baselining
- ☐ Insufficient strategic planning
- ☐ Inaccurate resource allocation
- ☐ Project delays

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Inadequate software baselining often results in project scope creep because functional requirements are not defined as well as they could be.

Question 209

Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

- ☐ Sensitive data can be read by operators.
- ☐ Data can be amended without authorization.
- ☒ Unauthorized report copies can be printed.
- ☐ Output can be lost in the event of system failure.

Explanation:

Explanation: Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operations. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

Question 210

What is the FIRST line of defense against criminal insider activities?

- ☐ Validating the integrity of personnel
- ☐ Monitoring employee activities
- ☐ Signing security agreements by critical personnel
- ☒ Stringent and enforced access controls

Question 211

A successful risk-based IT audit program should be based on:

- ☒ an effective scoring system.
- ☐ an effective PERT diagram.
- ☐ an effective departmental brainstorm session.
- ☐ an effective organization-wide brainstorm session.
- ☐ an effective yearly budget.
- ☐ None of the choices.

Explanation:

Explanation:

A successful risk-based IT audit program could be based on an effective scoring system. In establishing a scoring system, management should consider all relevant risk factors and avoid subjectivity. Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee.

Licensed to Berend Post berend.post@it-university.nl

Question 212

When an operating system is being hardened, it is MOST important for an information security manager to ensure that:

- ☒ default passwords are changed.
- ☐ anonymous access is removed.
- ☐ file access is restricted.
- ☐ system logs are activated.

Question 213

In a contract with a hot, warm or cold site, contractual provisions should cover which of the following considerations?

- ☐ Physical security measures
- ☐ Total number of subscribers
- ☒ Number of subscribers permitted to use a site at one time
- ☐ References by other users

Explanation:

Explanation:

The contract should specify the number of subscribers permitted to use the site at any one time. Physical security measures are not a part of the contract, although they are an important consideration when choosing a third-party site. The total number of subscribers is not a consideration; what is important is whether the agreement limits the number of subscribers in a building or in a specific area. The references that other users can provide is a consideration taken before signing the contract; it is by no means part of the contractual provisions.

Question 214

When an organization is having new software implemented under contract, which of the following is key to controlling escalating costs due to scope creep?

- ☐ Problem management
- ☒ Quality management
- ☐ Change management
- ☐ Risk management

Licensed to Berend Post berend.post@it-university.nl

Question 215

In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

- ☐ Disaster tolerance is high.
- ☐ Recovery time objective is high.
- ☒ Recovery point objective is low.
- ☐ Recovery point objective is high.

Explanation:

Explanation:

A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the data. If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of the disaster tolerance. The lower the RTO, the lower the disaster tolerance. Therefore, choice C is the correct answer.

Question 216

A purpose of project closure is to determine the:

- ☐ potential risks affecting the quality of deliverables.
- ☒ lessons learned for use in future projects.
- ☐ project feasibility requirements
- ☐ professional expertise of the project manager.

Question 217

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- ☐ User acceptance testing (UAT) occur for all reports before release into production
- ☒ Organizational data governance practices be put in place
- ☐ Standard software tools be used for report development
- ☐ Management sign-off on requirements for new reports

Explanation:

Explanation:

This choice directly addresses the problem. An organization wide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

Licensed to Berend Post berend.post@it-university.nl

Question 218

Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

Question 219

Which of the following is the MOST important reason for updating and retesting a business continuity plan?

- ☐ Staff turnover
- ☐ Emerging technology
- ☒ Significant business change
- ☐ Matching industry best practices

Question 220

The members of an emergency incident response team should be:

- ☒ selected from multiple departments
- ☐ assigned at the time of each incident
- ☐ restricted to IT personnel
- ☐ appointed by the CISO

Question 221

A post-implementation review of a system implementation has identified that the defined objectives were changed several times without the approval of the project board. What should the IS auditor do NEXT?

- ☐ Notify the project sponsor and request that the project be reopened.
- ☐ Ask management to obtain retrospective approvals.
- ☐ Notify the project management office and raise a finding.
- ☒ Determine whether the revised objectives are appropriate.

Licensed to Berend Post berend.post@it-university.nl

Question 222

When planning for the implementation of a new system, an organization will opt for a parallel run PRIMARILY to:

- ☐ ensure that the system meets required user response time.
- ☐ validate system processing.
- ☒ facilitate the training of new personnel.
- ☐ verify that system interfaces were implemented.

Question 223

After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

- ☐ Stress
- ☐ Black box
- ☐ Interface
- ☒ System

Explanation:

Explanation:

Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

Question 224

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- ☐ test data to validate data input.
- ☐ test data to determine system sort capabilities.
- ☒ generalized audit software to search for address field duplications.
- ☐ generalized audit software to search for account field duplications.

Explanation:

Explanation:

Since the name is not the same {due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

Licensed to Berend Post berend.post@it-university.nl

Question 225

Which of the following is an example of a passive attack initiated through the Internet?

- ☒ Traffic analysis
- ☐ Masquerading
- ☐ Denial of service
- ☐ E-mail spoofing

Explanation:

Explanation:

Internet security threats/vulnerabilities are divided into passive and active attacks. Examples of passive attacks include network analysis, eavesdropping and traffic analysis. Active attacks include brute force attacks, masquerading, packet replay, message modification, unauthorized access through the Internet or web-based services, denial-of-service attacks, dial-in penetration attacks, e-mail bombing and spamming, and e-mail spoofing.

Question 226

To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

- ☐ System access log files
- ☐ Enabled access control software parameters
- ☐ Logs of access control violations
- ☒ System configuration files for control options used

Explanation:

Explanation:

A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

Question 227

Which of the following will BEST protect the confidentiality of data stored on the hard drive of a laptop computer?

- ☒ Encryption of the data
- ☐ A boot password
- ☐ Physical locks and alarms
- ☐ Biometric access control

Licensed to Berend Post berend.post@it-university.nl

Question 228

An organization has implemented a distributed security administration system to replace the previous centralized one. The IS auditor's GREATEST concern should be that:

- ☒ security procedures may be inadequate to support the change.
- ☐ end-user acceptance of the new system is likely to be difficult to obtain.
- ☐ the new system will require additional training.
- ☐ a distributed security system is inherently a weak security system.

Question 229

When recommending a preventive control against cross-site scripting in web applications, an information security manager is MOST likely to suggest:

- ☐ using https in place of http.
- ☐ hardening of the web server's operating system.
- ☐ consolidating multiple sites into a single portal.
- ☒ coding standards and code review.

Question 230

By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

- ☐ reliable products are guaranteed.
- ☐ programmers' efficiency is improved.
- ☐ security requirements are designed.
- ☒ predictable software processes are followed.

Explanation:

Explanation:

By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

Licensed to Berend Post berend.post@it-university.nl

Question 231

For an auditor, it is very important to understand the different forms of project organization and their implication in the control of project management activities. In which of the following project organization form is management authority shared between the project manager and the department head?

- ☐ Influence project organization
- ☐ Pure project organization
- ☒ Matrix project organization
- ☐ Forward project organization

Explanation:

For CISA exam you should know the information below about Project Organizational Forms.

Three major forms of organizational alignment for project management within business organization are observe:

Influence project organization – The project manager has only a staff function without formal management authority. The project manager is only allowed to advise peers and team members as to which activities should be completed.

Pure project organization – The project manager has formal authority over those taking part in the project. Often this is bolstered by providing a special working area for the project team that is separated from their normal office space.

Matrix project organization – Management authority is shared between the project manager and the department head.

Request for the major project should be submitted to and prioritize by the IS steering committee. A project manager should be identified and appointed by the IS steering committee. The project manager, who need not be an IS staff member

The following were incorrect answers:

Influence project organization – The project manager has only a staff function without formal management authority. The project manager is only allowed to advise peers and team members as to which activities should be completed.

Pure project organization – The project manager has formal authority over those taking part in the project. Often this is bolstered by providing a special working area for the project team that is separated from their normal office space.

Licensed to Berend Post berend.post@it-university.nl

Forward project organization- Not a valid type of project organization form.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 148

Question 232

In what way is a common gateway interface (CGI) MOST often used on a webserver?

- ☒ Consistent way for transferring data to the application program and back to the user
- ☐ Computer graphics imaging method for movies and TV
- ☐ Graphic user interface for web design
- ☐ interface to access the private gateway domain

Explanation:

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orienteering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

Question 233

Which of the following would be the GREATEST risk associated with a new chat feature on a retailer's website?

- ☐ Productivity loss
- ☐ Reputational damage
- ☒ Data loss
- ☐ System downtime

Licensed to Berend Post berend.post@it-university.nl

Question 234

Which of the following is a risk of cross-training?

- ☐ Increases the dependence on one employee
- ☐ Does not assist in succession planning
- ☒ One employee may know all parts of a system
- ☐ Does not help in achieving a continuity of operations

Explanation:

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

Question 235

To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

- ☐ business software.
- ☐ infrastructure platform tools.
- ☒ application services.
- ☐ system development tools.

Explanation:

Explanation:

Projects should identify the complexities of the IT Infrastructure that can be simplified or isolated by the development of application services. Application services isolate system developers from the complexities of the IT infrastructure and offer common functionalities that are shared by many applications. Application services take the form of interfaces, middleware, etc. Business software focuses on business processes, whereas application services bridge the gap between applications and the IT Infrastructure components. Infrastructure platform tools are related to core hardware and software components required for development of the IT infrastructure. Systems development tools represent development components of the IT infrastructure development.

Licensed to Berend Post berend.post@it-university.nl

Question 236

Physical access controls are usually implemented based on which of the following means (Choose two.):

- ☒ mechanical locks
- ☒ guards
- ☐ operating systems
- ☐ transaction applications
- ☐ None of the choices.

Explanation:

Explanation:

In physical security, access control refers to the practice of restricting entrance to authorized persons. Human means of enforcement include guard, bouncer, receptionist ... etc. Mechanical means may include locks and keys.

Question 237

An IS auditor is asked to review a large organization's change management process. Which of the following practices presents the GREATEST risk?

- ☐ Emergency code changes are promoted without user acceptance testing.
- ☐ A system administrator performs code migration on planned downtime.
- ☒ Change management tickets do not contain specific documentation.
- ☐ Transaction data changes can be made by a senior developer.

Question 238

An integrated test facility is considered a useful audit tool because it:

- ☐ is a cost-efficient approach to auditing application controls.
- ☐ enables the financial and IS auditors to integrate their audit tests.
- ☒ compares processing output with independently calculated data.
- ☐ provides the IS auditor with a tool to analyze a large range of information

Explanation:

Explanation:

An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated data. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

Licensed to Berend Post berend.post@it-university.nl

Question 239

During audit planning, an IS auditor walked through the design of controls related to a new data loss prevention (DLP) tool. It was noted that the tool will be configured to alert IT management when large files are sent outside of the organization via email. What type of control will be tested?

- ☒ Detective
- ☐ Corrective
- ☐ Directive
- ☐ Preventive

Question 240

An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

- ☐ The data collected on attack methods
- ☐ The information offered to outsiders on the honeypot
- ☒ The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
- ☐ The risk that the honeypot would be subject to a distributed denial-of-service attack

Explanation:

Explanation:

Choice C represents the organizational risk that the honeypot could be used as a point of access to launch further attacks on the enterprise's systems. Choices A and B are purposes for deploying a honeypot, not a concern. Choice D, the risk that the honeypot would be subject to a distributed denial-of-service (DDoS) attack, is not relevant, as the honeypot is not a critical device for providing service.

Question 241

The FIRST step in a successful attack to a system would be:

- ☒ gathering information.
- ☐ gaining access.
- ☐ denying services.
- ☐ evading detection.

Explanation:

Explanation:

Successful attacks start by gathering information about the target system. This is done in advance so that the attacker gets to know the target systems and their vulnerabilities. All of the other choices are based on the information gathered.

Licensed to Berend Post berend.post@it-university.nl

Question 242

The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

- ☐ IT budget.
- ☐ existing IT environment.
- ☒ business plan.
- ☐ investment plan.

Explanation:

Explanation:

One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration. Choices A, B and D are important but secondary to the importance of reviewing the business plan,

Question 243

Which of the following testing procedure is used by the auditor during accounting audit to check errors in balance sheet and other financial documentation?

- ☐ Compliance testing
- ☐ Sanity testing
- ☐ Recovery testing
- ☒ Substantive testing

Explanation:

A procedure used during accounting audits to check for errors in balance sheets and other financial documentation. A substantive test might involve checking a random sample of transactions for errors, comparing account balances to find discrepancies, or analysis and review of procedures used to execute and record transactions.

Substantive testing is the stage of an audit when the auditor gathers evidence as to the extent of misstatements in client's accounting records or other information. This evidence is referred to as substantive evidence and is an important factor in determining the auditor's opinion on the financial statements as a whole. The audit procedures used to gather this evidence are referred to as substantive procedures, or substantive tests.

Substantive procedures (or substantive tests) are those activities performed by the auditor during the substantive testing stage of the audit that gather evidence as to the completeness, validity and/or accuracy of account balances and underlying classes of transactions.

Account balances and underlying classes of transaction must not contain any material misstatements. They must be materially complete, valid and accurate. Auditors gather evidence about these assertions by undertaking substantive procedures, which may include:

Licensed to Berend Post berend.post@it-university.nl

Physically examining inventory on balance date as evidence that inventory shown in the accounting records actually exists (validity assertion);

Arranging for suppliers to confirm in writing the details of the amount owing at balance date as evidence that accounts payable is complete (completeness assertion); and Making inquiries of management about the collectability of customers' accounts as evidence that trade debtors is accurate as to its valuation.

Evidence that an account balance or class of transaction is not complete, valid or accurate is evidence of a substantive misstatement.

The following answers are incorrect:

Compliance Testing - Compliance testing is basically an audit of a system carried out against a known criterion.

Sanity testing - Testing to determine if a new software version is performing well enough to accept it for a major testing effort. If application is crashing for initial use, then system is not stable enough for further testing and build or application is assigned to fix.

Recovery testing – Testing how well a system recovers from crashes, hardware failures, or other catastrophic problems.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 52 and 53

http://www.businessdictionary.com/definition/compliance-test.html

Question 244

IS audit is asked to explain how local area network (LAN) servers can contribute to a rapid dissemination of viruses. The IS auditor's BEST response is that:

- ☐ the server's software is the prime target and is the first to be infected.
- ☒ the server's operating system exchanges data with each station starting at every log-on.
- ☐ the server's file sharing function facilitates the distribution of files and applications.
- ☐ users of a given server have similar usage of applications and files.

Licensed to Berend Post berend.post@it-university.nl

Question 245

In a follow-up audit, an IS auditor notes that management has addressed the original findings in a different way than originally agreed upon. The auditor should FIRST:

- ☐ mark the recommendation as satisfied and close the finding
- ☐ verify if management's action mitigates the identified risk
- ☐ re-perform the audit to assess the changed control environment
- ☒ escalate the deviation to the audit committee

Question 246

What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality?

- ☒ Rapid application development (RAD)
- ☐ GANTT
- ☐ PERT
- ☐ Decision trees

Explanation:

Explanation: Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

Question 247

Identify the WAN message switching technique being used from the description presented below:

"Data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, this WAN switching technology stores and delays the message until ample resources become available for effective transmission of the message. "

- ☒ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Explanation:

For your exam you should know below information about WAN message transmission technique:

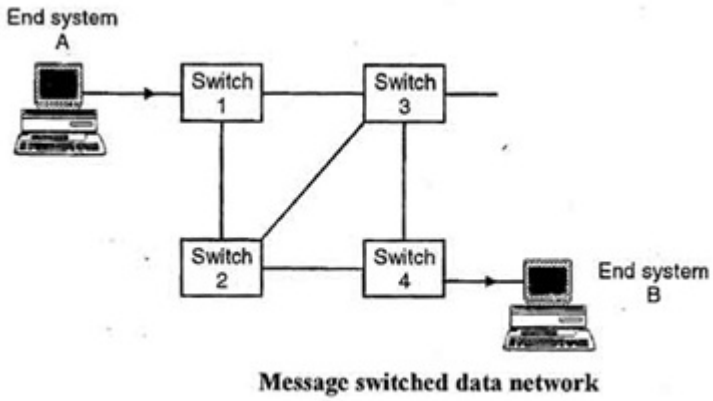
Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are

Licensed to Berend Post berend.post@it-university.nl

engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

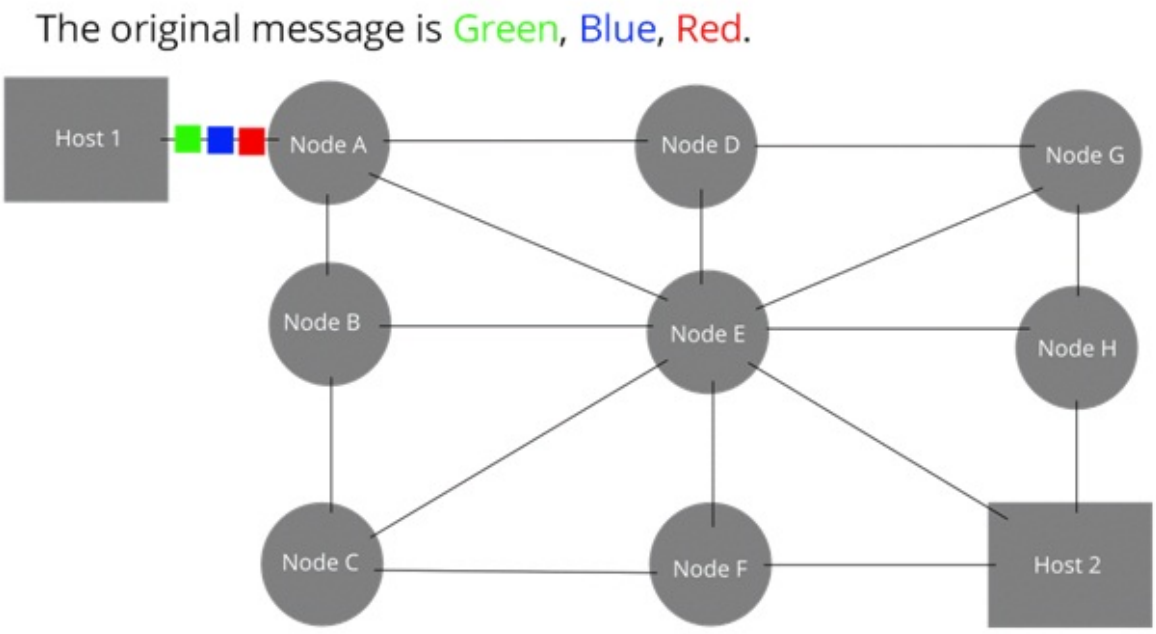


Message switched data network

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching



Licensed to Berend Post berend.post@it-university.nl

Circuit Switching

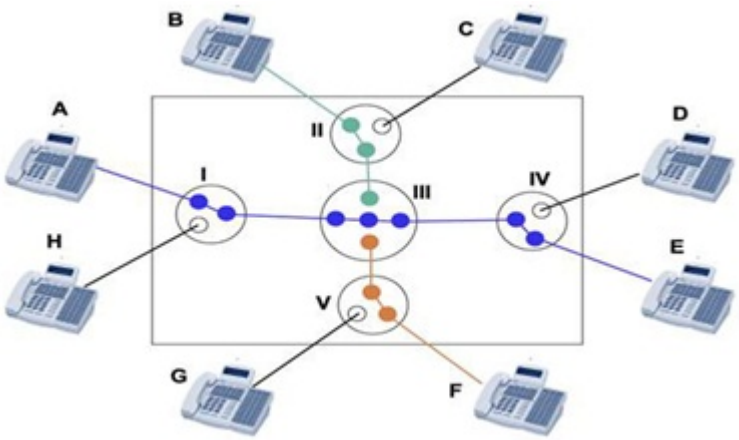
Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching



See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

Licensed to Berend Post berend.post@it-university.nl

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented are not valid choices.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

Licensed to Berend Post berend.post@it-university.nl

Question 248

COBIT 5 separates information goals into three sub-dimensions of quality. Which of the following sub-dimension of COBIT 5 describes the extent to which data values are in conformance with the actual true value?

- ☒ Intrinsic quality
- ☐ Contextual and representational quality
- ☐ Security quality
- ☐ Accessibility quality

Explanation:

Three sub-dimensions of quality in COBIT 5 are as follows:

1. Intrinsic quality – The extent to which data values are in conformance with the actual or true values. It includes

Accuracy – The extent to which information is correct or accurate and reliable

Objectivity – The extent to which information is unbiased, unprejudiced and impartial.

Believability – The extent to which information is regarded as true and credible.

Reputation – The extent to which information is highly regarded in terms of its source or content.

2. Contextual and Representational Quality – The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, reorganizing that information quality depends on the context of use. It includes

Relevancy – The extent to which information is applicable and helpful for the task at hand.

Completeness – The extent to which information is not missing and is of sufficient depth and breadth for the task at hand

Currency – The extent to which information is sufficiently up to date for task at hand.

Appropriate amount of information – The extent to which the volume of information is appropriate for the task at hand

Consistent Representation – The extent to which information is presented in the same format.

Interpretability – The extent to which information is in appropriate languages, symbols and units, with clear definitions.

Understandability - The extent to which information is easily comprehended.

Ease of manipulation – The extent to which information is easy to manipulate and apply to different tasks.

Licensed to Berend Post berend.post@it-university.nl

3. Security/accessibility quality – The extent to which information is available or obtainable. It includes:

Availability/timeliness – The extent to which information is available when required, or easily available when required, or easily and quickly retrievable.

Restricted Access – The extent to which access to information is restricted appropriately to authorize parties.

The following were incorrect answers:

Contextual and representational quality - The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, reorganizing that information quality depends on the context of use.

Security Quality or Accessibility quality -The extent to which information is available or obtainable.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 310

Question 249

The PRIMARY goal of a web site certificate is:

- ☒ authentication of the web site that will be surfed.
- ☐ authentication of the user who surfs through that site.
- ☐ preventing surfing of the web site by hackers.
- ☐ the same purpose as that of a digital certificate.

Explanation:

Explanation:

Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

Licensed to Berend Post berend.post@it-university.nl

Question 250

Which of the following is the MOST important reason for logging firewall activity?

- ☐ Intrusion detection
- ☒ Auditing purposes
- ☐ Firewall tuning
- ☐ Incident investigation

Question 251

Which of the following should be an IS auditor's PRIMARY concern when evaluating an organization's information security policies, procedures, and controls for third-party vendors?

- ☒ The third-party vendors have their own information security requirements.
- ☐ The organization is still responsible for protecting the data.
- ☐ Noncompliance is easily detected.
- ☐ The same procedures and controls are used for all third-party vendors.

Question 252

A multinational company wants to establish a mandatory global standard for information security including data protection and privacy. Which of the following should be the GREATEST concern to an IS auditor?

- ☐ Inconsistent roll-out of the standard across all countries.
- ☐ Increased organizational effort without any tangible benefit
- ☒ Noncompliance with local laws in the affected countries
- ☐ Lack of adoption by organized labor groups in all affected countries

Question 253

Which of the following E-commerce model covers all the transactions between companies and government organization?

- ☐ B-to-C relationships
- ☐ B-to-B relationships
- ☐ B-to-E relationships
- ☒ B-to-G relationships

Explanation:

Business-to-Government(B-to-G) relationships covers all the transactions between companies and government organizations. Currently this category is infancy, but it could expand quit rapidly as government use their own operations to promote awareness and growth of e-commerce. In addition to public procurement, administrations may also offer the option of electronic interchange for such transactions as VAT returns and the payment of corporate taxes.

Licensed to Berend Post berend.post@it-university.nl

For CISA exam you should know below E-commerce models:

Business-to-Consumer (B-to-C) relationships – The greatest potential power of E-commerce comes from its ability to redefine relationship with customers in creating a new convenient, low-cost channel to transact business. Companies can tailor their marketing strategies to an individual customer's needs and wants. As more of its business shifts on-line, a company will have an enhanced ability to track how its customer interact with it.

Business-to-Business (B-to-B) relationships -The relationship among the selling services of two or more business opens up the possibility of re-engineering business process across the boundaries that have traditionally separated external entities from each other. Because of the ease of access and the ubiquity of the Internet, for example companies can build business process that combine previously separated activities. The result is faster, higher quality and lower-cost set of transactions. The market has ever created to subdivision of B-to-B called business-to-small business(B-to-SB) relationships

Business-to-employee(B-to-E) relationships -Web technologies also assist in the dissemination of information to and among an organization employees.

Business-to-Government(B-to-G) relationships - covers all the transactions between companies and government organizations. Currently this category is infancy, but it could expand quit rapidly as government use their own operations to promote awareness and growth of e-commerce. In addition to public procurement, administrations may also offer the option of electronic interchange for such transactions as VAT returns and the payment of corporate taxes.

The following were incorrect answers:

The other options presented does not covers all transactions between companies and government organizations.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 175

Licensed to Berend Post berend.post@it-university.nl

Question 254

An IS auditor is performing a post-implementation review of a system deployed two years ago. Which of the following findings should be of MOST concern to the auditor?

- ☐ Maintenance costs were not included in the project lifecycle costs.
- ☒ Benefits as stated in the business case have not been realized.
- ☐ Workarounds due to remaining defects had to be used longer than anticipated.
- ☐ The system has undergone several change requests to further extend functionality.

Question 255

If concurrent update transactions to an account are not processed properly, which of the following will be affected?

- ☒ Integrity
- ☐ Confidentiality
- ☐ Availability
- ☐ Accountability

Question 256

During an audit, it is discovered that several suppliers with standing orders have been deleted from the supplier master file. Which of the following controls would have BEST prevented such an occurrence?

- ☒ Logical relationship check
- ☐ Existence check
- ☐ Table look-ups
- ☐ Referential integrity

Question 257

In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

- ☒ examine source program changes without information from IS personnel.
- ☐ detect a source program change made between acquiring a copy of the source and the comparison run.
- ☐ confirm that the control copy is the current version of the production program.
- ☐ ensure that all changes made in the current source copy are detected.

Explanation:

Explanation:

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately.

Licensed to Berend Post berend.post@it-university.nl

Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

Question 258

The MAIN consideration when designing an incident escalation plan should be ensuring that:

- ☐ information assets are classified.
- ☒ appropriate stakeholders are involved.
- ☐ high-impact risks have been identified.
- ☐ requirements cover forensic analysis.

Question 259

Which of the following tests is MOST likely to detect an error in one subroutine resulting from a recent change in another subroutine?

- ☐ Stress testing
- ☒ Regression testing
- ☐ User acceptance testing
- ☐ Black-box testing

Question 260

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- ☐ Personal firewall
- ☐ Antivirus programs
- ☒ Intrusion detection system (IDS)
- ☐ Virtual local area network (VLAN) configuration

Explanation:

Explanation:

An intrusion detection system (IDS) would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator. Antivirus programs, personal firewalls and VIAN configurations would be later in the line of defense.

Licensed to Berend Post berend.post@it-university.nl

Question 261

Which of the following is the PRIMARY objective of implementing privacy-related controls within an organization?

- ☐ To identify data at rest and data in transit for encryption
- ☐ To prevent confidential data loss
- ☒ To comply with legal and regulatory requirements
- ☐ To provide options to individuals regarding use of their data

Question 262

Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/IP model?

- ☐ Combines packets into bytes and bytes into frame
- ☒ Providers logical addressing which routers use for path determination
- ☐ Provide address to media using MAC address
- ☐ Performs only error detection

Explanation:

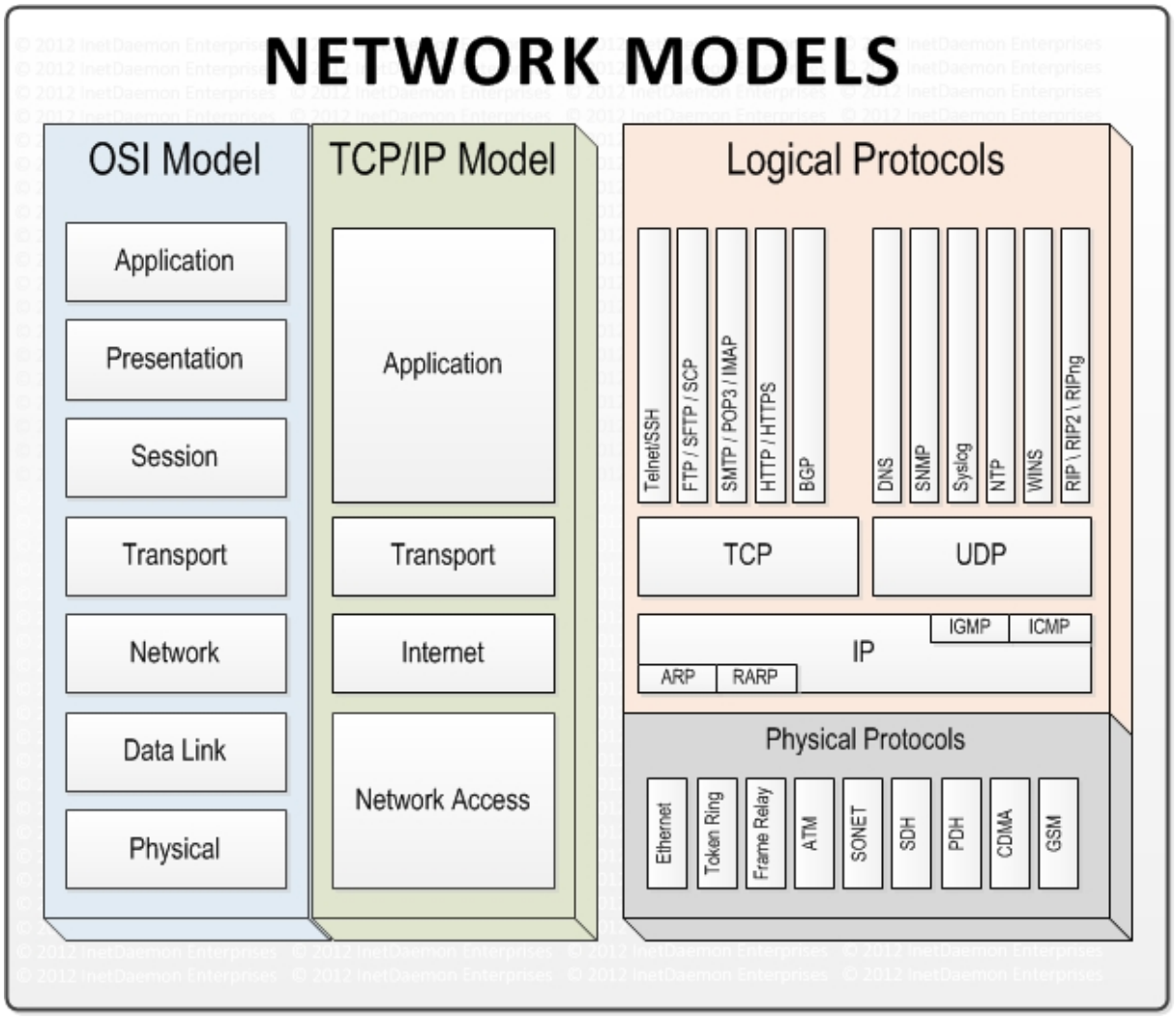
The word INCORRECTLY is the keyword used in the question. You need to find out the functionality that is not performed by LAN or WAN layer in TCP/IP model.

The Network layer of a TCP/IP model provides logical addressing which routers use for path determination.

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

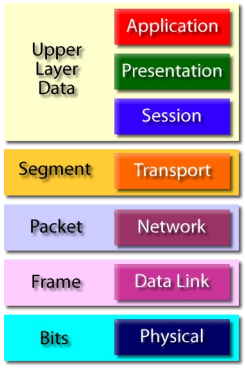
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe functionalities of application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 263

Which of the following provides the BEST single-factor authentication?

- ☒ Biometrics
- ☐ Password
- ☐ Token
- ☐ PIN

Explanation:

Explanation:

Although biometrics provides only single-factor authentication, many consider it to be an excellent method for user authentication.

Licensed to Berend Post berend.post@it-university.nl

Question 264

What process is used to validate a subject's identity?

- ☐ Identification
- ☐ Nonrepudiation
- ☐ Authorization
- ☒ Authentication

Explanation:

Explanation:

Authentication is used to validate a subject's identity.

Question 265

To help ensure the accuracy and completeness of end-user computing output, it is MOST important to include strong:

- ☒ reconciliation controls.
- ☐ change management controls.
- ☐ access management controls.
- ☐ documentation controls.

Question 266

Which of the following is a step in establishing a security policy?

- ☐ Developing platform-level security baselines.
- ☐ Developing configurations parameters for the network,
- ☒ Implementing a process for developing and maintaining the policy.
- ☐ Creating a RACI matrix.

Question 267

An organization plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

- ☐ Adequate storage space
- ☐ Complexity of administration
- ☐ Network bandwidth
- ☒ Application performance

Licensed to Berend Post berend.post@it-university.nl

Question 268

In a data center audit, an IS auditor finds that the humidity level is very low. The IS auditor would be MOST concerned because of an expected increase in:

- ☐ employee discomfort
- ☐ risk of fire
- ☒ static electricity problems
- ☐ backup tape failures

Question 269

What is an IS auditor's BEST course of action if informed by a business unit's representatives that they are too busy to cooperate with a scheduled audit?

- ☐ Reschedule the audit for a time more convenient to the business unit.
- ☒ Notify the chief audit executive who can negotiate with the head of the business unit.
- ☐ Begin the audit regardless and insist on cooperation from the business unit.
- ☐ Notify the audit committee immediately and request they direct the audit begin on schedule.

Question 270

Which of the following is the PRIMARY purpose of documenting and approving an information security policy?

- ☒ To communicate management's intent for securing the organization's information assets
- ☐ To mitigate the organization's information security risk to an acceptable level
- ☐ To ensure awareness of disciplinary procedures for security breaches by authorized users
- ☐ To determine the best approach for implementing information security within the organization

Question 271

A small startup organization does not have the resources to implement segregation of duties. Which of the following would be the MOST effective compensating control?

- ☐ Rotation of log monitoring and analysis responsibilities
- ☐ Additional management reviews and reconciliations
- ☐ Third-party assessments
- ☒ Mandatory vacations

Explanation:

Reference:https://www.computerweekly.com/tip/Segregation-of-duties-Small-business-best-practices

Licensed to Berend Post berend.post@it-university.nl

Question 272

Which of the following is the PRIMARY reason an IS auditor should discuss observations with management before delivering a final report?

- ☐ Identify business risks associated with the observations.
- ☐ Assist the management with control enhancements.
- ☐ Record the proposed course of corrective action.
- ☒ Validate the audit observations.

Question 273

Which of the following is the BEST way to identify the potential impact of a successful attack on an organization's mission critical applications?

- ☐ Execute regular vulnerability scans
- ☒ Conduct penetration testing
- ☐ Perform an application vulnerability review
- ☐ Perform an independent code review

Question 274

When reviewing business continuity plan (BCP) test results, it is MOST important for the IS auditor to determine whether the test:

- ☒ verifies the ability to resume key business operations.
- ☐ considers changes to the systems environment.
- ☐ assesses the capability to retrieve vital records.
- ☐ follows up on activities that occurred since the previous test.

Question 275

Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

- ☐ A program that deposits a virus on a client machine
- ☐ Applets recording keystrokes and, therefore, passwords
- ☐ Downloaded code that reads files on a client's hard drive
- ☒ Applets opening connections from the client machine

Explanation:

Explanation:

An applet is a program downloaded from a web server to the client, usually through a web browser that provides functionality for database access, interactive web pages and communications with other users. Applets opening connections from the client machine to other machines on the network and damaging those machines, as a denial-of-service attack, pose the greatest threat to an

Licensed to Berend Post berend.post@it-university.nl

organization and could disrupt business continuity. A program that deposits a virus on a client machine is referred to as a malicious attack (i.e., specifically meant to cause harm to a client machine), but may not necessarily result in a disruption of service. Applets that record keystrokes, and therefore, passwords, and downloaded code that reads files on a client's hard drive relate more to organizational privacy issues, and although significant, are less likely to cause a significant disruption of service.

Question 276

Data flow diagrams are used by IS auditors to:

- ☐ order data hierarchically.
- ☐ highlight high-level data definitions.
- ☒ graphically summarize data paths and storage.
- ☐ portray step-by-step details of data generation.

Explanation:

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

Question 277

In a large organization, IT deadlines on important projects have been missed because IT resources are not prioritized properly. Which of the following is the BEST recommendation to address this problem?

- ☒ Implement project portfolio management.
- ☐ Implement an integrated resource management system.
- ☐ Implement a comprehensive project scorecard.
- ☐ Revisit the IT strategic plan.

Question 278

The FIRST course of action an investigator should take when a computer is being attacked is to:

- ☐ terminate all active processes.
- ☐ copy the contents of the hard drive.
- ☒ disconnect it from the network.
- ☐ disconnect the power source.

Licensed to Berend Post berend.post@it-university.nl

Question 279

If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

- ☐ IT cannot be implemented if senior management is not committed to strategic planning.
- ☐ More likely.
- ☒ Less likely.
- ☐ Strategic planning does not affect the success of a company's implementation of IT.

Explanation:

Explanation:

A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

Question 280

A database administrator (DBA) extracts a user listing for an auditor as testing evidence. Which of the following will provide the GREATEST assurance that the user listing is reliable?

- ☐ Requesting a query that returns the count of the users.
- ☐ Requesting a copy of the query that generated the user listing
- ☐ Obtaining sign-off from the DBA to attest that the list is complete
- ☒ Witnessing the DBA running the query in-person

Question 281

Which of the following provides the BEST audit evidence that a firewall is configured in compliance with the organization's security policy?

- ☐ Analyzing how the configuration changes are performed
- ☒ Performing penetration testing
- ☐ Analyzing log files
- ☐ Reviewing the rule base

Question 282

An IS auditor finds that confidential company data has been inadvertently leaked through social engineering. The MOST effective way to help prevent a recurrence of this issue is to implement:

- ☐ penalties to staff for security policy breaches.
- ☐ a third-party intrusion prevention solution.
- ☒ a security awareness program.
- ☐ data loss prevention (DLP) software.

Licensed to Berend Post berend.post@it-university.nl

Question 283

Which of the following is the BEST indication of a successful information security culture?

- ☐ Penetration testing is done regularly and findings remediated.
- ☒ End users know how to identify and report incidents.
- ☐ Individuals are given access based on job functions.
- ☐ The budget allocated for information security is sufficient.

Question 284

A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

- ☐ recommend that the project be halted until the issues are resolved.
- ☐ recommend that compensating controls be implemented.
- ☒ evaluate risks associated with the unresolved issues.
- ☐ recommend that the project manager reallocate test resources to resolve the issues.

Explanation:

Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choices might be appropriate only after the risks have been assessed.

Question 285

An IS auditor should recommend the use of library control software to provide reasonable assurance that:

- ☒ program changes have been authorized.
- ☐ only thoroughly tested programs are released.
- ☐ modified programs are automatically moved to production.
- ☐ source and executable code integrity is maintained.

Explanation:

Explanation:

Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

Licensed to Berend Post berend.post@it-university.nl

Question 286

When evaluating the ability of a disaster recovery plan to enable the recovery of IT processing capabilities, it is MOST important for the IS auditor to verify the plan is:

- ☐ stored at an offsite location
- ☐ communicated to department heads
- ☒ regularly reviewed
- ☐ periodically tested

Question 287

An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

- ☐ Simple Object Access Protocol (SOAP)
- ☒ Address Resolution Protocol (ARP)
- ☐ Routing Information Protocol (RIP)
- ☐ Transmission Control Protocol (TCP)

Explanation:

Explanation:

Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform- independent XML- based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connection and exchange streams of data.

Question 288

Due to the small size of the payroll department, an organization is unable to segregate the employee setup and payroll processing functions. Which of the following would be the BEST compensating control for the lack of segregation of duties?

- ☐ An independent payroll disbursement review is conducted.
- ☐ The system is configured to require secondary approval for changes to the employee master file.
- ☐ A review is conducted to verify that terminated employees are removed from the employee master file.
- ☒ A payroll variance report is reviewed for anomalies every pay period.

Licensed to Berend Post berend.post@it-university.nl

Question 289

Following the discovery of inaccuracies in a data warehouse, an organization has implemented data profiling, cleansing, and handling filters to enhance the quality of data obtained from connected sources. Which type of control has been applied?

- ☐ Preventive control
- ☒ Corrective control
- ☐ Compensating control
- ☐ Detective control

Question 290

Which of the following statement INCORRECTLY describes anti-malware?

- ☐ 2
- ☐ 3
- ☐ 2 and 3
- ☒ None of the choices listed

Explanation:

The word INCORRECT is the keyword used in the question. All the terms presented in options correctly describes some type of anti-malware related activities.

For your exam you should know below mentioned different kinds of malware Controls

A. Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

Licensed to Berend Post berend.post@it-university.nl

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other types of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

E. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

The following were incorrect answers:

All of the choices presented other than one were describing Anti-Malware related activities

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 354 and 355

Licensed to Berend Post berend.post@it-university.nl

Question 291

An IS auditor notes that application of super-user activity was not recorded in system logs. What is the auditor's BEST course of action?

- ☐ Recommend a least-privilege access model.
- ☒ Investigate the reason for the lack of logging.
- ☐ Report the issue to the audit manager.
- ☐ Recommend activation of super-user activity logging.

Question 292

An IS auditor is reviewing a software-based configuration. Which of the following represents the GREATEST vulnerability? The firewall software:

- ☐ is configured with an implicit deny rule as the last rule in the rule base.
- ☒ is installed on an operating system with default settings.
- ☐ has been configured with rules permitting or denying access to systems or networks.
- ☐ is configured as a virtual private network (VPN) endpoint.

Explanation:

Explanation:

Default settings are often published and provide an intruder with predictable configuration information, which allows easier system compromise. To mitigate this risk, firewall software should be installed on a system using a hardened operating system that has limited functionality, providing only the services necessary to support the firewall software. Choices A, C and D are normal or best practices for firewall configurations.

Question 293

During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

- ☒ Evacuation plan
- ☐ Recovery priorities
- ☐ Backup storages
- ☐ Call tree

Explanation:

Explanation:

Protecting human resources during a disaster-related event should be addressed first. Having separate BCPs could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients. Choices B, C and D may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.

Licensed to Berend Post berend.post@it-university.nl

Question 294

Which of the following would be of MOST concern during an audit of an end user computing system containing sensitive information?

- ☐ Audit logging is not available.
- ☒ System data is not protected.
- ☐ Secure authorization is not available.
- ☐ The system is not included in inventory.

Question 295

The PRIMARY purpose of vulnerability assessments is to:

- ☒ detect deficiencies that could lead to a system compromise.
- ☐ provide clear evidence that the system is sufficiently secure.
- ☐ test intrusion detection systems (IDS) and response procedures.
- ☐ determine the impact of potential threats.

Question 296

Which of the following would help to ensure the completeness of batch file transfers?

- ☐ Input controls
- ☐ Self-checking digits
- ☒ Hash totals
- ☐ Parity check

Question 297

An e-commerce enterprise's disaster recovery (DR) site has 30% less processing capability than the primary site. Based on this information, which of the following presents the GREATEST risk?

- ☐ Network firewalls and database firewalls at the DR site do not provide high availability.
- ☐ No disaster recovery plan (DRP) testing has been performed during the last six months.
- ☐ The DR site is in a shared location that hosts multiple other enterprises.
- ☒ The DR site has not undergone testing to confirm its effectiveness.

Licensed to Berend Post berend.post@it-university.nl

Question 298

When developing a business continuity plan (BCP), which of the following should be performed FIRST?

- ☐ Develop business continuity training
- ☐ Classify operations
- ☒ Conduct a business impact analysis (BIA)
- ☐ Establish a disaster recovery plan (DRP)

Question 299

Which of the following method of expressing knowledge base consist of a graph in which nodes represent physical or conceptual objects and the arcs describes the relationship between nodes?

- ☐ Decision tree
- ☐ Rules
- ☒ Semantic nets
- ☐ Knowledge interface

Explanation:

Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

For CISA Exam you should know below information about Artificial Intelligence and Expert System

Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used

Goals are generated and achieved

Information is communicated

Collaboration is achieved

Concepts are formed

Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.

Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Licensed to Berend Post berend.post@it-university.nl

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degrees Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

Knowledge interface – Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule - Expressing declarative knowledge through the use of if-then relationships.

Semantic nets - Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 187

Question 300

Which of the following audit combines financial and operational audit steps?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☒ Integrated Audit
- ☐ Forensic audit

Explanation:

Explanation:

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

For your exam you should know below information about different types of audit:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization's accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be

Licensed to Berend Post berend.post@it-university.nl

backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits

Licensed to Berend Post berend.post@it-university.nl

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance Audit - A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and

Licensed to Berend Post berend.post@it-university.nl

risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Financial Audit- A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Forensic Audit - Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

Licensed to Berend Post berend.post@it-university.nl

Question 301

Which of the following types of attack involves a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files?

- ☒ Local DoS attacks
- ☐ Remote DoS attacks
- ☐ Distributed DoS attacks
- ☐ Local Virus attacks
- ☐ None of the choices.

Explanation:

Explanation:

Local DoS attacks can be a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files. The best defense is to find this program and kill it.

Question 302

An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

- ☐ The network security group can change network address translation (NAT).
- ☐ There are conflicting permit and deny rules for the IT group.
- ☐ There is only one rule per group with access privileges.
- ☒ Individual permissions are overriding group permissions.

Question 303

Which of the following is MOST important for an IS auditor to evaluate when determining the effectiveness of an information security program?

- ☐ Percentage of users aware of the objectives of the security program
- ☐ Percentage of policy exceptions that were approved with justification
- ☒ Percentage of desired control objectives achieved
- ☐ Percentage of reported security incidents

Question 304

A large chain of shops with electronic funds transfer (EFT) at point-of-sale devices has a central communications processor for connecting to the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?

- ☐ Offsite storage of daily backups
- ☐ Alternative standby processor onsite
- ☐ installation of duplex communication links
- ☒ Alternative standby processor at another network node

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Having an alternative standby processor at another network node would be the best solution. The unavailability of the central communications processor would disrupt all access to the banking network, resulting in the disruption of operations for all of the shops. This could be caused by failure of equipment, power or communications. Offsite storage of backups would not help, since EFT tends to be an online process and offsite storage will not replace the dysfunctional processor. The provision of an alternate processor onsite would be fine if it were an equipment problem, but would not help in the case of a power outage, installation of duplex communication links would be most appropriate if it were only the communication link that failed.

Question 305

Doing which of the following during peak production hours could result in unexpected downtime?

- ☐ Performing data migration or tape backup
- ☒ Performing preventive maintenance on electrical systems
- ☐ Promoting applications from development to the staging environment
- ☐ Replacing a failed power supply in the core router of the data center

Explanation:

Explanation:

Choices A and C are processing events which may impact performance, but would not cause downtime. Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenance activities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

Question 306

Which of the following is the most important element in the design of a data warehouse?

- ☒ Quality of the metadata
- ☐ Speed of the transactions
- ☐ Volatility of the data
- ☐ Vulnerability of the system

Explanation:

Explanation:

Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

Licensed to Berend Post berend.post@it-university.nl

Question 307

During a review of information security procedures for disabling user accounts, an IS auditor discovers that IT is only disabling network access for terminated employees. IT management maintains if terminated users cannot access the network, they will not be able to access any applications. Which of the following is the GREATEST risk associated with application access?

- ☐ Unauthorized access to data
- ☐ Inability to access data
- ☐ Lack of segregation of duties
- ☒ Loss of non-repudiation

Question 308

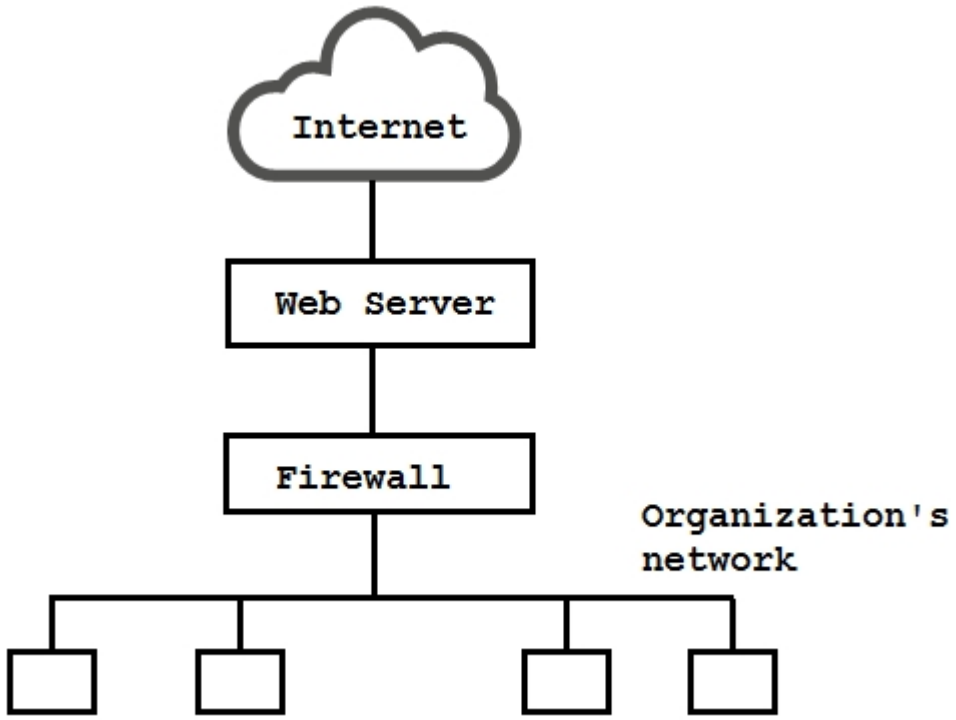
An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

- ☒ Abuses by employees have not been reported.
- ☐ Vulnerabilities have not been properly addressed.
- ☐ Security incident policies are out of date.
- ☐ Lessons learned have not been properly documented.

Licensed to Berend Post berend.post@it-university.nl

Question 309

To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



- ☒ Firewall and the organization's network.
- ☐ Internet and the firewall.
- ☐ Internet and the web server.
- ☐ Web server and the firewall.

Explanation:

Explanation:

Attack attempts that could not be recognized by the firewall will be detected if a network- based intrusion detection system is placed between the firewall and the organization's network. A network-based intrusion detection system placed between the internet and the firewall will detect attack attempts, whether they do or do not enter the firewall.

Question 310

Which of the following is MOST influential when defining disaster recovery strategies?

- ☐ Existing server redundancies
- ☒ Maximum tolerable downtime
- ☐ Data classification scheme
- ☐ Annual loss expectancy

Licensed to Berend Post berend.post@it-university.nl

Question 311

IS management has decided to install a level 1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:

- ☐ upgrading to a level 5 RAID.
- ☐ increasing the frequency of onsite backups.
- ☒ reinstating the offsite backups.
- ☐ establishing a cold site in a secure location.

Explanation:

Explanation:

A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups, more frequent onsite backups or even setting up a cold site. Choices A, B and D do not compensate for the lack of offsite backup.

Question 312

Which of the following is the BEST way to help ensure the security of privacy-related data stored by an organization?

- ☒ Encrypt personally identifiable information (PII).
- ☐ Publish the data classification scheme.
- ☐ Inform data owners of the purpose of collecting information.
- ☐ Classify privacy-related data as confidential.

Question 313

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

- ☐ An organizational certificate
- ☐ A user certificate
- ☒ A website certificate
- ☐ Authenticode

Explanation:

Explanation:

A website certificate is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption.

Licensed to Berend Post berend.post@it-university.nl

Question 314

The MOST critical security weakness of a packet level firewall is that it can be circumvented by:

- ☐ using a dictionary attack of encrypted passwords.
- ☒ changing the source address on incoming packets.
- ☐ intercepting packets and viewing passwords sent in clear text.
- ☐ deciphering the signature information of the packets.

Question 315

Which of the following is the initial step in creating a firewall policy?

- ☐ A cost-benefit analysis of methods for securing the applications
- ☒ Identification of network applications to be externally accessed
- ☐ Identification of vulnerabilities associated with network applications to be externally accessed
- ☐ Creation of an applications traffic matrix showing protection methods

Explanation:

Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

Question 316

An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

- ☐ adequate fire insurance exists.
- ☐ regular hardware maintenance is performed.
- ☒ offsite storage of transaction and master files exists.
- ☐ backup processing facilities are fully tested.

Explanation:

Explanation:

Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

Licensed to Berend Post berend.post@it-university.nl

Question 317

Which of the following is the BEST way to achieve high availability and fault tolerance for an e-business system?

- ☐ Network diversity
- ☐ Storage area network
- ☒ Robust systems architecture
- ☐ Secure offsite backup storage

Question 318

To create a digital signature in a message using asymmetric encryption, it is necessary to:

- ☐ first use a symmetric algorithm for the authentication sequence.
- ☒ encrypt the authentication sequence using a public key.
- ☐ transmit the actual digital signature in unencrypted clear text.
- ☐ encrypt the authentication sequence using a private key.

Question 319

The use of digital signatures:

- ☐ requires the use of a one-time password generator.
- ☐ provides encryption to a message.
- ☒ validates the source of a message.
- ☐ ensures message confidentiality.

Explanation:

Explanation:

The use of a digital signature verifies the identity of the sender, but does not encrypt the whole message, and hence is not enough to ensure confidentiality. A one-time password generator is an option, but is not a requirement for using digital signatures.

Question 320

The MOST effective control for reducing the risk related to phishing is:

- ☐ centralized monitoring of systems.
- ☐ including signatures for phishing in antivirus software.
- ☐ publishing the policy on antiphishing on the intranet.
- ☒ security training for all users.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Phishing is a type of e-mail attack that attempts to convince a user that the originator is genuine, with the intention of obtaining information. Phishing is an example of a social engineering attack. Any social engineering type of attack can best Decontrolled through security and awareness training.

Question 321

Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

- ☐ Presentation layer
- ☐ Desktop Access Layer
- ☒ Data Mart layer
- ☐ Data access layer

Explanation:

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

Licensed to Berend Post berend.post@it-university.nl

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are

 Licensed to Berend Post berend.post@it-university.nl

counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Licensed to Berend Post berend.post@it-university.nl

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 322

Which of the following backup schemes is the BEST option when storage media is limited?

- ☐ Virtual backup
- ☐ Real-time backup
- ☒ Differential backup
- ☐ Full backup

Question 323

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- ☐ address of the domain server.
- ☒ resolution service for the name/address.
- ☐ IP addresses for the internet.
- ☐ domain name system.

Explanation:

Explanation:

DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Licensed to Berend Post berend.post@it-university.nl

Question 324

Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

- ☒ The alternate facility will be available until the original information processing facility is restored.
- ☐ User management is involved in the identification of critical systems and their associated critical recovery times.
- ☐ Copies of the plan are kept at the homes of key decision-making personnel.
- ☐ Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Explanation:

Explanation:

The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or the execution pf the plan.

Question 325

A 5-year audit plan provides for general audits every year and application audits on alternating years. To achieve higher efficiency, the IS audit manager would MOST likely:

- ☐ proceed with the plan and integrate all new applications.
- ☐ alternate between control self-assessment (CSA) and general audits every year.
- ☐ implement risk assessment criteria to determine audit priorities.
- ☒ have control self-assessments (CSAs) and formal audits of applications on alternating years.

Question 326

Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☒ TCP

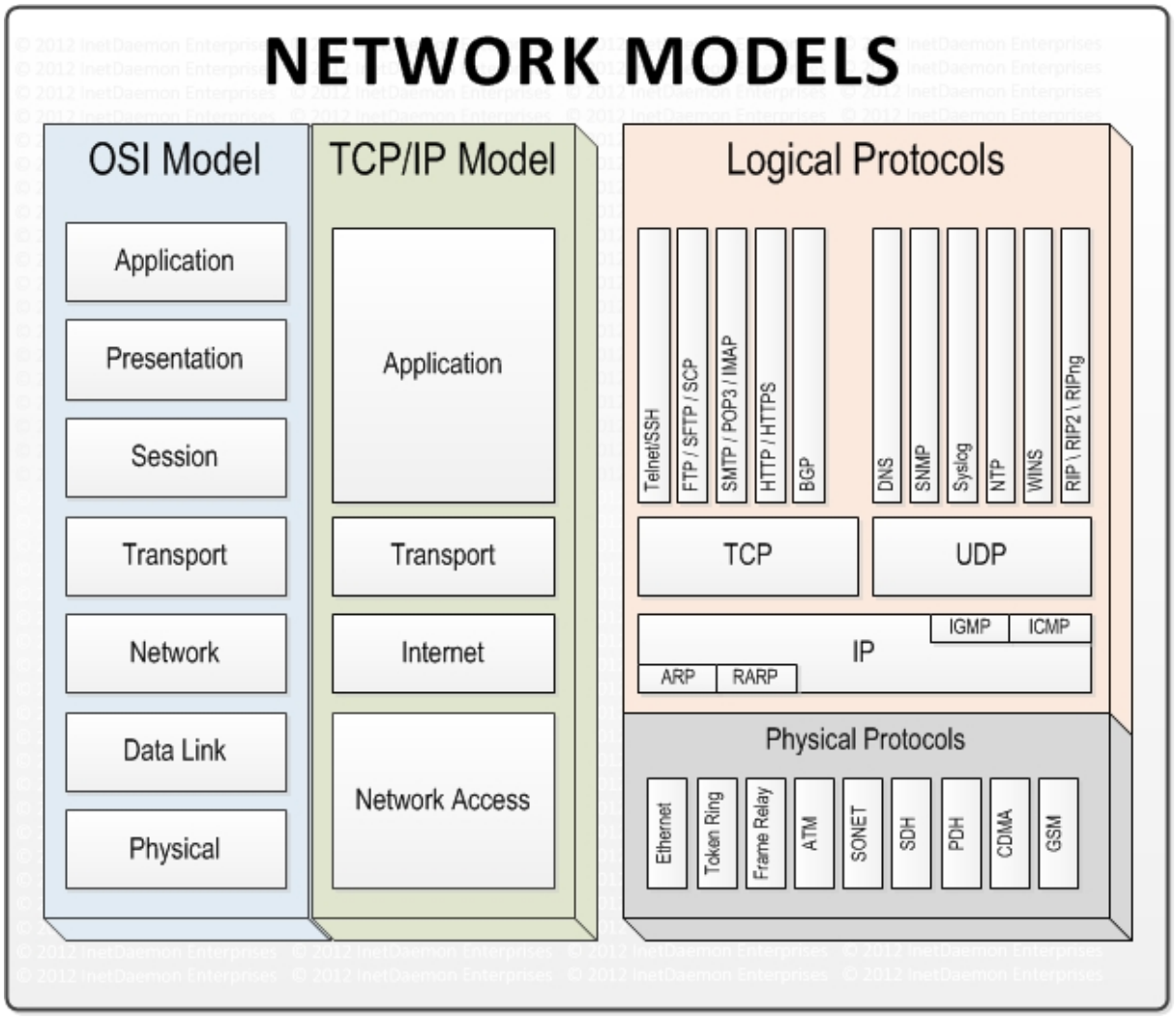
Explanation:

The NOT keyword is used in the question. You need to find out a protocol which does not work at application layer. TCP protocol works at transport layer of a TCP/IP models.

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

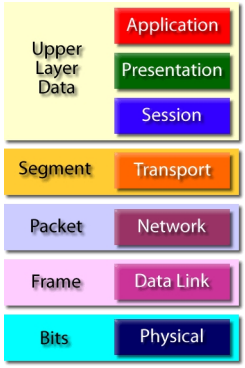
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if

Licensed to Berend Post berend.post@it-university.nl

two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):

Protocol Data Unit - PDU



The following answers are incorrect:

HTTP, FTP and NTP protocols works at application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 327

An organization was severely impacted after an advanced persistent threat (APT) attack. Afterwards, it was found that the initial breach happened a month prior to the attack. Management's GREATEST concern should be:

- ☐ results of the past internal penetration test
- ☒ the effectiveness of monitoring processes
- ☐ the installation of critical security patches
- ☐ external firewall policies

Licensed to Berend Post berend.post@it-university.nl

Question 328

An internal audit department recently established a quality assurance (QA) program as part of its overall audit program. Which of the following activities is MOST important to include as part of the QA program requirements?

- ☒ Implementing corrective action plans.
- ☐ Reviewing audit standards periodically
- ☐ Analyzing user satisfaction reports from business lines
- ☐ Creating a long-term plan for internal audit staffing

Question 329

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

- ☐ dependency on a single person.
- ☐ inadequate succession planning.
- ☒ one person knowing all parts of a system.
- ☐ a disruption of operations.

Explanation:

Explanation:

Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

Question 330

An organization has agreed to perform remediation related to high risk audit findings. The remediation process involves a complex reorganization of user roles as well as the implementation of several compensating controls that may not be completed within the next audit cycle. Which of the following is the BEST way for an IS auditor to follow up on the activities?

- ☐ Review the progress of remediation on a regular basis.
- ☒ Provide management with a remediation timeline and verify adherence.
- ☐ Continue to audit the failed controls according to the audit schedule.
- ☐ Schedule a review of the controls after the projected remediation date.

Licensed to Berend Post berend.post@it-university.nl

Question 331

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

- ☒ Applications may not be subject to testing and IT general controls
- ☐ increased development and maintenance costs
- ☐ increased application development time
- ☐ Decision-making may be impaired due to diminished responsiveness to requests for information

Explanation:

Explanation:

End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls, quality assurance procedures, and documentation. A risk of end-user applications is that management may rely on them as much as traditional applications. End-user computing (EUC) systems typically result in reduced application development and maintenance costs, and a reduced development cycle time. EUC systems normally increase flexibility and responsiveness to management's information requests.

Question 332

As part of a post-implementation review, the BEST way to assess the realization of outcomes is by:

- ☒ obtaining feedback from the user community.
- ☐ performing a comprehensive risk analysis.
- ☐ evaluating the actual performance of the system.
- ☐ comparing the business case benefits to the archived benefits.

Question 333

During a privileged access review, an IS auditor observes many help desk employees have privileges within systems not required for their job functions. Implementing which of the following would have prevented this situation?

- ☐ Separation of duties
- ☐ Multi-factor authentication
- ☒ Least privilege access
- ☐ Privileged access reviews

Licensed to Berend Post berend.post@it-university.nl

Question 334

Which of the following provides the BEST assurance that security policies are applied across business operations?

- ☐ Organizational standards are required to be formally accepted.
- ☐ Organizational standards are enforced by technical controls.
- ☐ Organizational standards are included in awareness training.
- ☒ Organizational standards are documented in operational procedures.

Question 335

Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

- ☐ a firewall exists.
- ☐ a secure web connection is used.
- ☒ the source of the executable file is certain.
- ☐ the host web site is part of the organization.

Explanation:

Explanation:

Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere. It is virtually impossible at this time to filter at this level. A secure web connection or firewall is considered an external defense. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither a secure web connection nor a firewall can identify an executable file as friendly. Hosting the web site as part of the organization is impractical. Enabling the acceptance of Java applets and/or Active X controls is an all-or- nothing proposition. The client will accept the program if the parameters are established to do so.

Question 336

Which of the following is the BEST source of information for assessing the effectiveness of IT process monitoring?

- ☐ Participative management techniques
- ☐ Quality assurance (QA) reviews
- ☒ Performance data
- ☐ Real-time audit software

Licensed to Berend Post berend.post@it-university.nl

Question 337

An organization has software that is not compliant with data protection requirements. To help ensure that appropriate and relevant data protection controls are implemented in the future, the auditor's BEST course of action would be to:

☒ conduct a privacy impact assessment to identity gaps in the organization's privacy.
☐ recommend that privacy checks are included within the solution development life cycle.
☐ recommend an executive be appointed to oversee privacy program improvements.
☐ map the organization's business processes to identify personally identifiable information (PII).

Question 338

The specific advantage of white box testing is that it:

☐ verifies a program can operate successfully with other parts of the system.
☐ ensures a program's functional operating effectiveness without regard to the internal program structure.
☒ determines procedural accuracy or conditions of a program's specific logic paths.
☐ examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Explanation:

Explanation:

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

Question 339

An employee uses a personal mobile device to access corporate data and email, but also allows friends to use it as a mobile hotspot for Internet access when not at work. The information security manager is concerned this situation may expose confidential data. The manager's FIRST step should be to:

☒ update the mobile device usage standards to address the issue and communicate to all employees
☐ activate the incident response plan to mitigate the impact and stop the compromise
☐ review the associated risks to determine if additional controls are needed
☐ implement additional security controls that will mitigate the situation and then reassess risks

Licensed to Berend Post berend.post@it-university.nl

Question 340

In the event of a data center disaster, which of the following would be the MOST appropriate strategy to enable a complete recovery of a critical database?

- ☐ Daily data backup to tape and storage at a remote site
- ☒ Real-time replication to a remote site
- ☐ Hard disk mirroring to a local server
- ☐ Real-time data backup to the local storage area network (SAN)

Explanation:

Explanation:

With real-time replication to a remote site, data are updated simultaneously in two separate locations; therefore, a disaster in one site would not damage the information located in the remote site. This assumes that both sites were not affected by the disaster. Daily tape backup recovery could lose up to a day's work of data. Choices C and D take place in the same data center and could possibly be affected by the same disaster.

Question 341

A new system development project is running late against a critical implementation deadline. Which of the following is the MOST important activity?

- ☐ Document last-minute enhancements.
- ☐ Perform user acceptance testing.
- ☐ Perform a pre-implementation audit.
- ☒ Ensure that code has been reviewed.

Question 342

When evaluating whether the expected benefits of a project have been achieved, it is MOST important for an IS auditor to review:

- ☐ post-implementation issues.
- ☐ quality assurance results.
- ☐ the project schedule.
- ☒ the business case.

Licensed to Berend Post berend.post@it-university.nl

Question 343

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- ☐ O/S and hardware refresh frequencies
- ☒ Gain-sharing performance bonuses
- ☐ Penalties for noncompliance
- ☐ Charges tied to variable cost metrics

Explanation:

Explanation:

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

Question 344

An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

- ☐ documentation of staff background checks.
- ☒ independent audit reports or full audit access.
- ☐ reporting the year-to-year incremental cost reductions.
- ☐ reporting staff turnover, development or training.

Explanation:

Explanation:

When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

Licensed to Berend Post berend.post@it-university.nl

Question 345

Which of the following is a type of computer network used for data transmission among devices such as computers, telephones and personal digital assistants?

- ☐ LAN
- ☐ WAN
- ☒ SAN
- ☐ PAN

Question 346

During a follow-up audit, an IS auditor learns the organization implemented an automated process instead of the originally agreed upon enhancement of the manual process. The auditor should:

- ☐ report the finding that recommendations were not acted upon
- ☐ perform a cost-benefit analysis on the new process
- ☒ verify that the new process satisfies control objectives
- ☐ report the recommendation as implemented

Question 347

Which of the following is MOST helpful in preventing a systems failure from occurring when an application is replaced using the abrupt changeover technique?

- ☐ Comprehensive documentation
- ☐ Comprehensive testing
- ☐ Threat and risk assessment
- ☒ Change management

Question 348

Which of the following types of controls would be MOST important to implement when digitizing human resource (HR) records?

- ☒ Change management controls
- ☐ Software development controls
- ☐ Project management controls
- ☐ Access management controls

Licensed to Berend Post berend.post@it-university.nl

Question 349

An IS auditor is observing transaction processing and notes that a high-priority update job ran out of sequence. What is the MOST significant risk from this observation?

- ☐ Previous jobs may have failed.
- ☐ The job may not have run to completion.
- ☐ Daily schedules may not be accurate.
- ☒ The job competes with invalid data.

Question 350

To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

- ☒ the entire message and thereafter enciphering the message digest using the sender's private key.
- ☐ any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.
- ☐ the entire message and thereafter enciphering the message using the sender's private key.
- ☐ the entire message and thereafter enciphering the message along with the message digest using the sender's private key.

Explanation:

Explanation:

A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the sender's private key, not the message.

Question 351

Intrusion detection systems (IDSs) can:

- ☐ substitute for a firewall.
- ☐ compensate for weak authentication mechanisms.
- ☐ conduct investigations of attacks from within the network.
- ☒ provide information to enhance the security infrastructure.

Licensed to Berend Post berend.post@it-university.nl

Question 352

Performance monitoring tools report that servers are consistently above the recommended utilization capacity. Which of the following is the BEST recommendation of the IS auditor?

- ☒ Develop a capacity plan based on usage projections.
- ☐ Deploy load balancers.
- ☐ Monitor activity logs.
- ☐ Add servers until utilization is at target capacity.

Question 353

In a typical SDLC, which group is PRIMARILY responsible for confirming compliance with requirements?

- ☐ Steering committee
- ☐ Risk management
- ☒ Quality assurance
- ☐ Internal audit

Question 354

Code changes are compiled and placed in a change folder by the developer. An implementation team migrates changes to production from the change folder. Which of the following BEST indicates separation of duties is in place during the migration process?

- ☒ A second individual performs code review before the change is released to production.
- ☐ The developer approves changes prior to moving them to the change folder.
- ☐ The implementation team does not have experience writing code.
- ☐ The implementation team does not have access to change the source code.

Question 355

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

- ☐ recovery.
- ☒ retention.
- ☐ rebuilding.
- ☐ reuse.

Explanation:

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the official form of classic 'paper* makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the

Licensed to Berend Post berend.post@it-university.nl

property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

Question 356

Which of the following strategies BEST optimizes data storage without compromising data retention practices?

- ☐ Limiting the size of the file attachments being sent via email
- ☐ Automatically deleting emails older than one year
- ☒ Moving emails to a virtual email vault after 30 days
- ☐ Allowing employees to store large emails on flash drives

Question 357

Which of the following is the MOST important prerequisite for implementing a data loss prevention (DLP) tool?

- ☐ Identifying where existing data resides and establishing a data classification matrix.
- ☐ Requiring users to save files in secured folders instead of a company-wide shared drive
- ☐ Reviewing data transfer logs to determine historical patterns of data flow
- ☒ Developing a DLP policy and requiring signed acknowledgement by users

Question 358

When continuous monitoring systems are being implemented, an IS auditor should FIRST identify:

- ☐ the location and format of output files
- ☐ applications that provide the highest financial risk
- ☐ high-risk areas within the organization
- ☒ the controls on which to focus

Question 359

The use of object-oriented design and development techniques would MOST likely:

- ☒ facilitate the ability to reuse modules.
- ☐ improve system performance.
- ☐ enhance control effectiveness.
- ☐ speed up the system development life cycle.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

One of the major benefits of object-oriented design and development is the ability to reuse modules. The other options do not normally benefit from the object-oriented technique.

Question 360

Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files.

- ☐ Confidentiality
- ☐ Integrity
- ☒ Redundancy
- ☐ Concurrency

Explanation:

Explanation: Redundancy is the best answer because it provides both integrity and availability. Organizations should use off-site storage facilities to maintain redundancy of current and critical information within backup files.

Question 361

The responsibility for authorizing access to a business application system belongs to the:

- ☒ data owner.
- ☐ security administrator.
- ☐ IT security manager.
- ☐ requestor's immediate supervisor.

Explanation:

Explanation:

When a business application is developed, the best practice is to assign an information or data owner to the application. The Information owner should be responsible for authorizing access to the application itself or to back-end databases for queries. Choices B and C are not correct because the security administrator and manager normally do not have responsibility for authorizing access to business applications. The requestor's immediate supervisor may share the responsibility for approving user access to a business application system; however, the final responsibility should go to the information owner.

Licensed to Berend Post berend.post@it-university.nl

Question 362

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

- ☐ IS auditor
- ☐ Database administrator
- ☐ Project manager
- ☒ Data owner

Explanation:

Explanation:

During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted data. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated data. A project manager provides day-to- day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

Question 363

Which of the following is the FIRST step in initiating a data classification program?

- ☐ Risk appetite assessment
- ☐ Inventory of data assets
- ☒ Assignment of data ownership
- ☐ Assignment of sensitivity levels

Explanation:

Explanation:

The data classification process starts with the process of establishing ownership of data. This process also helps to prepare data dictionary

Question 364

What is the MOST difficult aspect of access control in a multiplatform, multiple-site client/server environment?

- ☐ Creating new user IDs valid only on a few hosts
- ☒ Maintaining consistency throughout all platforms
- ☐ Restricting a local user to necessary resources on a local platform
- ☐ Restricting a local user to necessary resources on the host server

Licensed to Berend Post berend.post@it-university.nl

Question 365

Which of the following type of computer is a large, general purpose computer that are made to share their processing power and facilities with thousands of internal or external users?

- ☐ Thin client computer
- ☐ Midrange servers
- ☐ Personal computers
- ☒ Mainframe computers

Explanation:

Mainframe computer is a large, general purpose computer that are made to share their processing power and facilities with thousands of internal or external users. The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are

Licensed to Berend Post berend.post@it-university.nl

measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers

A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers

A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1] They are also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a mice (microphone) pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as ultra-books or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Licensed to Berend Post berend.post@it-university.nl

Smartphone, tablets and other handheld devices

A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard.

A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers. Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Thin Client computers

A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following answers are incorrect:

Mid-range servers- Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM).

Personal computers - A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and

 Licensed to Berend Post berend.post@it-university.nl

mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Thin Client computers- A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 246

http://en.wikipedia.org/wiki/Thin_client

http://en.wikipedia.org/wiki/Mobile_device

http://en.wikipedia.org/wiki/Personal_computer

http://en.wikipedia.org/wiki/Classes_of_computers

http://en.wikipedia.org/wiki/Laptop

Question 366

The BEST reason for implementing a virtual private network (VPN) is that it:

- ☐ eases the implementation of data encryption.
- ☐ allows for public use of private networks.
- ☐ enables use of existing hardware platforms.
- ☒ allows for private use of public networks.

Explanation:

Explanation:

Virtual private networks (VPNs) connect remote users over an insecure public network such as the Internet. The connection is virtual because it is temporary with no physical presence. VPN technology is cost-effective and highly flexible. A VPN creates an encrypted tunnel to securely pass data as follows:

Between two machines (host-host)

From a machine to a network (host-gateway)

From one network to another network (gateway-gateway)

Licensed to Berend Post berend.post@it-university.nl

Question 367

What can be implemented to provide the highest level of protection from external attack?

- ☒ Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- ☐ Configuring the firewall as a screened host behind a router
- ☐ Configuring the firewall as the protecting bastion host
- ☐ Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Explanation:

Explanation:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

Question 368

Which of the following methods BEST ensures that a comprehensive approach is used to direct information security activities?

- ☐ Creating communication channels
- ☒ Promoting security training
- ☐ Establishing a steering committee
- ☐ Holding periodic meetings with business owners

Question 369

The MOST important difference between hashing and encryption is that hashing:

- ☒ is irreversible.
- ☐ output is the same length as the original message.
- ☐ is concerned with integrity and security.
- ☐ is the same at the sending and receiving end.

Explanation:

Explanation:

Hashing works one way; by applying a hashing algorithm to a message, a message hash/digest is created. If the same hashing algorithm is applied to the message digest, it will not result in the original message. As such, hashing is irreversible, while encryption is reversible. This is the basic difference between hashing and encryption. Hashing creates an output that is smaller than the original message, and encryption creates an output of the same length as the original message. Hashing is used to verify the integrity of the message and does not address security. The same hashing algorithm is used at the sending and receiving ends to generate and verify the message hash/digest. Encryption will not necessarily use the same algorithm at the sending and receiving and to encrypt and decrypt.

Licensed to Berend Post berend.post@it-university.nl

Question 370

In the context of effective information security governance, the primary objective of value delivery is to:

- ☒ optimize security investments in support of business objectives.
- ☐ implement a standard set of security practices.
- ☐ institute a standards-based solution.
- ☐ implement a continuous improvement culture.

Explanation:

Explanation:

In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

Question 371

Which of the following is a passive attack on a network?

- ☐ Message service interruption
- ☐ Message modification
- ☒ Traffic analysis
- ☐ Sequence analysis

Question 372

In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

- ☐ isolation.
- ☐ consistency.
- ☒ atomicity.
- ☐ durability.

Explanation:

Explanation:

The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions; hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been

Licensed to Berend Post berend.post@it-university.nl

reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

Question 373

Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

- ☐ verify compatibility with the hot site.
- ☐ Review the implementation report.
- ☐ Perform a walk-through of the disaster recovery plan.
- ☒ Update the IS assets inventory.

Explanation:

Explanation:

An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to update the disaster recovery plan after having updated the required assets inventory.

Question 374

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- ☐ implementation.
- ☐ compliance.
- ☐ documentation.
- ☒ sufficiency.

Explanation:

Explanation:

An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

Licensed to Berend Post berend.post@it-university.nl

Question 375

A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

- ☐ The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
- ☒ The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
- ☐ The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
- ☐ The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

Explanation:

Explanation:

It is a common mistake to use scenario planning for business continuity. The problem is that it is impossible to plan and document actions for every possible scenario. Planning for just selected scenarios denies the fact that even improbable events can cause an organization to break down. Best practice planning addresses the four possible areas of impact in a disaster: premises, people, systems, and suppliers and other dependencies. All scenarios can be reduced to these four categories and can be handled simultaneously. There are very few special scenarios which justify an additional separate analysis, it is a good idea to use best practices and external advice for such an important topic, especially since knowledge of the right level of preparedness and the judgment about adequacy of the measures taken is not available in every organization. The recovery time objectives (RTOs) are based on the essential business processes required to ensure the organization's survival, therefore it would be inappropriate for them to be based on IT capabilities. Best practice guidelines recommend having 20%-40% of normal capacity available at an emergency site; therefore, a value of 50% would not be a problem if there are no additional factors.

Question 376

Library control software restricts source code to:

- ☒ Read-only access
- ☐ Write-only access
- ☐ Full access
- ☐ Read-write access

Explanation:

Explanation: Library control software restricts source code to read-only access.

Licensed to Berend Post berend.post@it-university.nl

Question 377

An organization has created a policy that defines the types of web sites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

- ☐ Stateful inspection firewall
- ☒ Web content filter
- ☐ Web cache server
- ☐ Proxy server

Explanation:

Explanation:

A web content filter accepts or denies web communications according to the configured rules. To help the administrator properly configure the tool, organizations and vendors have made available URL blacklists and classifications for millions of web sites. A stateful inspection firewall is of little help in filtering web traffic since it does not review the content of the web site nor does it take into consideration the sites classification. A web cache server is designed to improve the speed of retrieving the most common or recently visited web pages. A proxy server is incorrect because a proxy server is a server which services the request of its clients by forwarding requests to other servers. Many people incorrectly use proxy server as a synonym of web proxy server even though not all web proxy servers have content filtering capabilities.

Question 378

Which of the following should be of MOST concern to an IS auditor during the review of a quality management system?

- ☐ The quality management system includes training records for IT personnel.
- ☒ There are no records to document actions for minor business processes.
- ☐ Important quality checklists are maintained outside the quality management system.
- ☐ Indicators are not fully represented in the quality management system.

Question 379

The MOST effective way to determine if IT is meeting business requirements is to establish:

- ☐ industry benchmarks.
- ☐ organizational goals.
- ☐ a capability model.
- ☒ key performance indicators (KPIs).

Licensed to Berend Post berend.post@it-university.nl

Question 380

When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?

- ☐ Report distribution
- ☐ Encryption
- ☒ Tuning
- ☐ Retention

Question 381

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organization's information security manager?

- ☐ The operations team implemented the change without regression testing.
- ☒ The change did not include a proper assessment of risk.
- ☐ Documentation of the change was made after implementation.
- ☐ The information security manager did not review the change prior to implementation.

Question 382

A financial institution that processes millions of transactions each day has a central communications processor (switch) for connecting to automated teller machines (ATMs). Which of the following would be the BEST contingency plan for the communications processor?

- ☐ Reciprocal agreement with another organization
- ☐ Alternate processor in the same location
- ☒ Alternate processor at another network node
- ☐ Installation of duplex communication links

Explanation:

Explanation:

The unavailability of the central communications processor would disrupt all access to the banking network. This could be caused by an equipment, power or communications failure. Reciprocal agreements make an organization dependent on the other organization and raise privacy, competition and regulatory issues. Having an alternate processor in the same location resolves the equipment problem, but would not be effective if the failure was caused by environmental conditions (i.e., power disruption). The installation of duplex communication links would only be appropriate if the failure were limited to the communication link.

Licensed to Berend Post berend.post@it-university.nl

Question 383

Which of the following is a form of Hybrid Cryptography where the sender encrypts the bulk of the data using Symmetric Key cryptography and then communicates securely a copy of the session key to the receiver?

- ☒ Digital Envelope
- ☐ Digital Signature
- ☐ Symmetric key encryption
- ☐ Asymmetric

Explanation:

A Digital Envelope is used to send encrypted information using symmetric keys, and the relevant session key along with it. It is a secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key, which is used to encrypt the bulk of the date or message can be referred to as session key. It is simply a symmetric key picked randomly in the key space.

In order for the receiver to have the ability to decrypt the message, the session key must be sent to the receiver.

This session key cannot be sent in clear text to the receiver, it must be protected while in transit, else anyone who have access to the network could have access to the key and confidentiality can easily be compromised.

Therefore, it is critical to encrypt and protect the session key before sending it to the receiver. The session key is encrypted using receiver's public key. Thus providing confidentiality of the key.

The encrypted message and the encrypted session key are bundled together and then sent to the receiver who, in turn opens the session key with the receiver matching private key.

The session key is then applied to the message to get it in plain text.

The process of encrypting bulk data using symmetric key cryptography and encrypting the session key with a public key algorithm is referred as a digital envelope. Sometimes people refer to it as Hybrid Cryptography as well.

The following were incorrect answers:

Digital-signature – A digital signature is an electronic identification of a person or entity created by using public key algorithm and intended to verify to recipient the integrity of the data and the identity of the sender. Applying a digital signature consist of two simple steps, first you create a

Licensed to Berend Post berend.post@it-university.nl

message digest, then you encrypt the message digest with the sender's private key. Encrypting the message digest with the private key is the act of signing the message.

Symmetric Key Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

Asymmetric Key Encryption - The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric") cryptography which relies on the same key to perform both. Public-key algorithms are based on mathematical problems which currently admit no efficient solution that are inherent in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is computationally easy for a user to generate their own public and private key-pair and to use them for encryption and decryption. The strength lies in the fact that it is "impossible" (computationally unfeasible) for a properly generated private key to be determined from its corresponding public key. Thus the public key may be published without compromising security, whereas the private key must not be revealed to anyone not authorized to read messages or perform digital signatures. Public key algorithms, unlike symmetric key algorithms, do not require a secure initial exchange of one (or more) secret keys between the parties.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 350 and 351

http://en.wikipedia.org/wiki/Public-key_cryptography

Question 384

Establishing the level of acceptable risk is the responsibility of:

- ☐ quality assurance management.
- ☒ senior business management.
- ☐ the chief information officer.
- ☐ the chief security officer.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.

Question 385

Which of the following would BEST support 24/7 availability?

- ☐ Daily backup
- ☐ offsite storage
- ☒ Mirroring
- ☐ Periodic testing

Explanation:

Explanation:

Mirroring of critical elements is a too! that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

Question 386

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☒ MTD

Explanation:

Explanation:

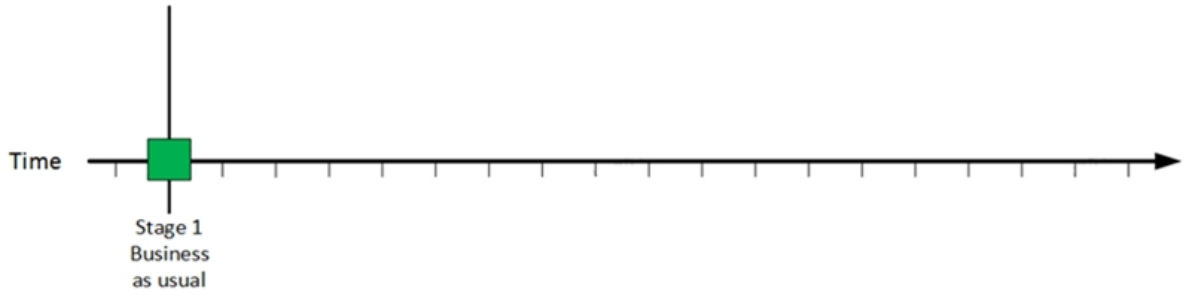
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

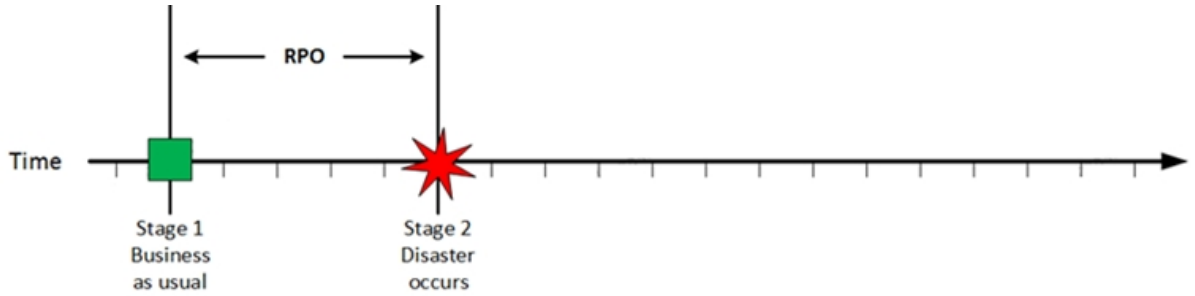
Licensed to Berend Post berend.post@it-university.nl



At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

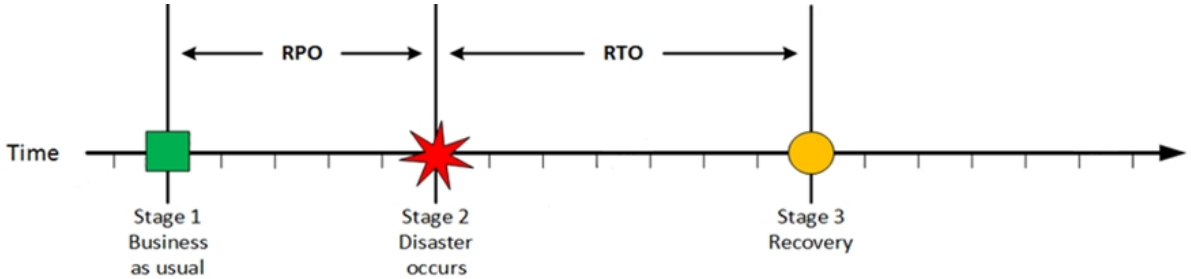
Disaster Occurs



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

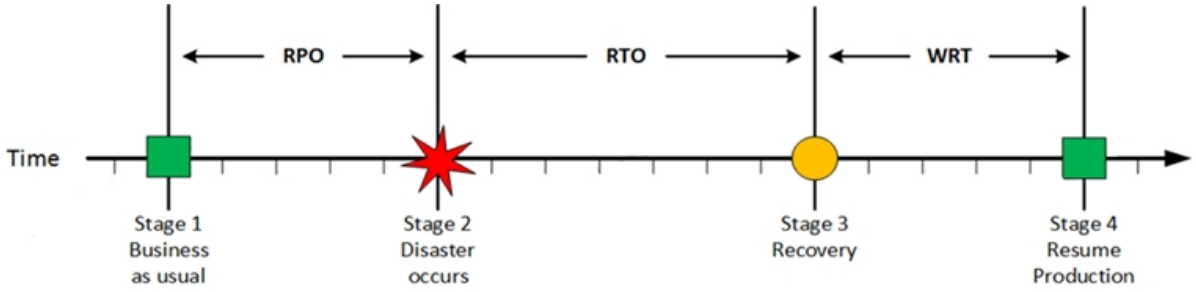


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Licensed to Berend Post berend.post@it-university.nl

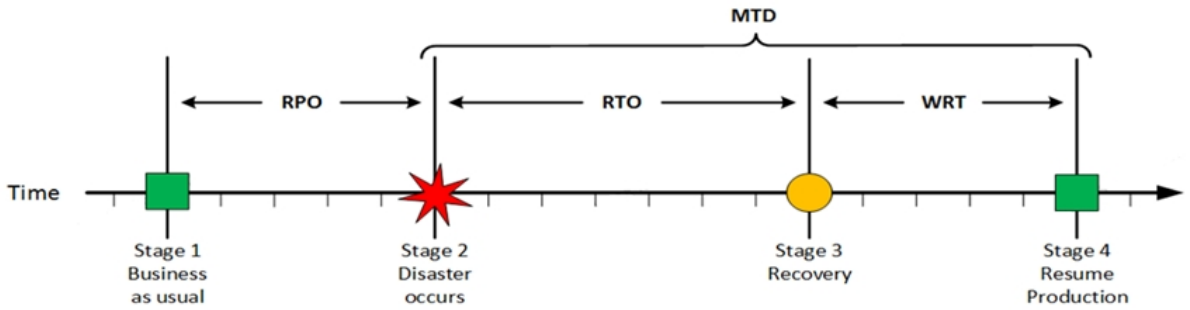
Stage 4: Resume Production

Resume Production



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Licensed to Berend Post berend.post@it-university.nl

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

References:

CISA review manual 2014 page number 284

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 387

Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?

- ☐ Execute access to development program libraries
- ☐ Write access to development data libraries
- ☐ Execute access to production program libraries
- ☒ Write access to production program libraries

Question 388

What is a common vulnerability, allowing denial-of-service attacks?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Lack of employee awareness of organizational security policies
- ☒ Improperly configured routers and router access lists
- ☐ Configuring firewall access rules

Explanation:

Explanation:

Improperly configured routers and router access lists are a common vulnerability for denial-of-service attacks.

 Licensed to Berend Post berend.post@it-university.nl

Question 389

The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

- ☐ alignment of the IT activities with IS audit recommendations.
- ☒ enforcement of the management of security risks.
- ☐ implementation of the chief information security officer's (CISO) recommendations.
- ☐ reduction of the cost for IT security.

Explanation:

Explanation:

The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risks. Recommendations, visions and objectives of the auditor and the chief information security officer (CISO) are usually included within a security program, but they would not be the major benefit.

The cost of IT security may or may not be reduced.

Question 390

Attribute sampling is BEST suited to estimate:

- ☐ compliance with approved procedures.
- ☐ the true monetary value of a population.
- ☐ the total error amount in the population.
- ☒ whether a recorded balance is within limits of materiality.

Question 391

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

- ☐ Establishing an inter-networked system of client servers with suppliers for increased efficiencies
- ☐ Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
- ☒ Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
- ☐ Reengineering the existing processing and redesigning the existing system

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

EDI is the best answer. Properly implemented (e.g., agreements with trading partner's transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

Question 392

To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:

- ☒ established guidelines.
- ☐ overall IT capacity and operational constraints.
- ☐ efficient technical processing considerations.
- ☐ criteria consistent with classification levels.

Question 393

Why is it not preferable for a firewall to treat each network frame or packet in isolation?

- ☒ Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- ☐ Such a firewall is costly to setup.
- ☐ Such a firewall is too complicated to maintain.
- ☐ Such a firewall is CPU hungry.
- ☐ Such a firewall offers poor compatibility.
- ☐ None of the choices.

Explanation:

Explanation:

A stateless firewall treats each network frame or packet in isolation.

Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

Question 394

Which of the following is used in providing logical access control to restrict updating or deleting business information in a relational database?

- ☐ Trigger
- ☒ View
- ☐ Join
- ☐ Primary key

Licensed to Berend Post berend.post@it-university.nl

Question 395

Which of the following IS functions can be performed by the same group or individual while still providing the proper segregation of duties?

- ☒ Computer operations and application programming
- ☐ Database administration and computer operations
- ☐ Security administration and application programming
- ☐ Application programming and systems analysis

Explanation:

Reference: https://www.isaca.org/Journal/archives/2016/volume-3/Pages/implementing-segregation-of-duties.aspx

Question 396

Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization's incident management processes?

- ☐ Metrics are not reported to senior management.
- ☐ Service management standards are not followed.
- ☐ Expected time to resolve incidents is not specified.
- ☒ Prioritization criteria are not defined.

Question 397

The reason for establishing a stop or freezing point on the design of a new system is to:

- ☐ prevent further changes to a project in process.
- ☐ indicate the point at which the design is to be completed.
- ☒ require that changes after that point be evaluated for cost-effectiveness.
- ☐ provide the project management team with more control over the project design.

Explanation:

Explanation:

Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost- benefits and the payback period.

Licensed to Berend Post berend.post@it-university.nl

Question 398

What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information?

- ☒ Referential integrity controls
- ☐ Normalization controls
- ☐ Concurrency controls
- ☐ Run-to-run totals

Explanation:

Explanation:

Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

Question 399

A computer program used by multiple departments has data quality issues. There is no agreement as to who should be responsible for corrective action. Which of the following is an IS auditor's BEST course of action?

- ☐ Recommend the IT department be assigned data cleansing responsibility.
- ☐ Modify the program to automatically cleanse the data and close the issue.
- ☐ Assign responsibility to the primary department using the program.
- ☒ Note the disagreement and recommend establishing data governance.

Question 400

John has been hired to fill a new position in one of the well-known financial institute. The position is for IS auditor. He has been assigned to complete IS audit of one of critical financial system. Which of the following should be the first step for John to be perform during IS audit planning?

- ☐ Perform risk assessment
- ☒ Determine the objective of the audit
- ☐ Gain an understanding of the business process
- ☐ Assign the personnel resource to audit

Explanation:

Determine the objective of audit should be the first step in the audit planning process. Depending upon the objective of an audit, auditor can gather the information about business process.

For CISA exam you should know the information below:

Steps to perform audit planning

Licensed to Berend Post berend.post@it-university.nl

Gain an understanding of the business mission, objectives, purpose and processes which includes information and processing requirement such as availability, integrity, security and business technology and information confidentiality.

Understand changes in the business environment audited.

Review prior work papers

Identify stated contents such as policies, standards and required guidelines, procedure and organization structures.

Perform a risk analysis to help in designing the audit plan.

Set the audit scope and audit objectives.

Develop the audit approach or audit strategy

Assign personnel resources to audit

Address engagement logistics.

The following answers are incorrect:

The other options specified should be completed once we finalize on the objective of audit.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 30 (The process of auditing information system)

Question 401

Which of the following ACID property in DBMS requires that each transaction is "all or nothing"?

- ☒ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Explanation:

Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

For CISA exam you should know below information about ACID properties in DBMS:

Licensed to Berend Post berend.post@it-university.nl

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction. [citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

The following were incorrect answers:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

Question 402

During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

- ☐ responsibility for maintaining the business continuity plan.
- ☐ criteria for selecting a recovery site provider.
- ☒ recovery strategy.
- ☐ responsibilities of key personnel.

Explanation:

Explanation:

The most appropriate strategy is selected based on the relative risk level and criticality identified in the business impact analysis (BIA.) The other choices are made after the selection or design of the appropriate recovery strategy.

Question 403

An IS auditor is mapping controls to risk for an accounts payable system. What is the BEST control to detect errors in the system?

- ☐ Alignment of the process to business objectives
- ☐ Quality control review of new payments
- ☐ Management approval of payments
- ☒ Input validation

Question 404

Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

- ☐ Function point analysis
- ☐ Critical path methodology
- ☒ Rapid application development
- ☐ Program evaluation review technique

Explanation:

Explanation:

Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The program evaluation review technique (PERT) and critical path methodology (CPM) are both

Licensed to Berend Post berend.post@it-university.nl

planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

Question 405

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

- ☐ Process maturity
- ☐ Performance indicators
- ☒ Business risk
- ☐ Assurance reports

Explanation:

Explanation:

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

Question 406

While reviewing an organization's business continuity plan (BCP), an IS auditor observes that a recently developed application is not included. The IS auditor should:

- ☒ ensure that the criticality of the application is determined.
- ☐ ignore the observation as the application is not mission critical.
- ☐ include in the audit findings that the BCP is incomplete.
- ☐ recommend that the application be incorporated in the BCP.

Question 407

Which of the following do digital signatures provide?

- ☒ Authentication and integrity of data
- ☐ Authentication and confidentiality of data
- ☐ Confidentiality and integrity of data
- ☐ Authentication and availability of data

Explanation:

Explanation:

The primary purpose of digital signatures is to provide authentication and integrity of data.

Licensed to Berend Post berend.post@it-university.nl

Question 408

An internal IS auditor discovers that a service organization did not notify its customers following a data breach. Which of the following should the auditor do FIRST?

- ☒ Notify audit management of the finding.
- ☐ Report the finding to regulatory authorities.
- ☐ Notify the service organization's customers.
- ☐ Require the service organization to notify its customers.

Question 409

Which of the following weaknesses would have the GREATEST impact on the effective operation of a perimeter firewall?

- ☐ Ad-hoc monitoring of firewall activity
- ☐ Potential back doors to the firewall software
- ☒ Misconfiguration on the firewall rules
- ☐ Use of stateful firewalls with default configuration

Question 410

An organization which uses external cloud services extensively is concerned with risk monitoring and timely response. The BEST way to address this concern is to ensure:

- ☒ the availability of continuous technical support
- ☐ internal security standards are in place
- ☐ a right-to-audit clause is included in contracts
- ☐ appropriate service level agreements (SLAs) are in place

Question 411

Which of the following should be the PRIMARY objective of an information security governance framework?

- ☐ Increase the organization's return on security investment.
- ☒ Provide a baseline for optimizing the security profile of the organization.
- ☐ Ensure that users comply with the organization's information security policies.
- ☐ Demonstrate compliance with industry best practices to external stakeholders.

Licensed to Berend Post berend.post@it-university.nl

Question 412

The BEST way to assure an organization's board of directors that IT strategies support business objectives is to:

- ☐ provide regular assessments of emerging technologies
- ☒ identify and report on the achievement of critical success factors
- ☐ confirm that IT strategies have been fully documented and disseminated
- ☐ ensure that senior business managers review IT budgets

Question 413

An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. The information security manager's BEST course of action should be to:

- ☐ modify the policy
- ☒ present the risk to senior management
- ☐ enforce the policy
- ☐ create an exception for the deviation

Question 414

In computer forensic which of the following describe the process that converts the information extracted into a format that can be understood by investigator?

- ☒ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☐ Extraction

Explanation:

Investigation is the process that converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Licensed to Berend Post berend.post@it-university.nl

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.

Be able to withstand a barrage of legal security

Be unambiguous and not open to misinterpretation.

Be easily referenced

Contains all information required to explain conclusions reached

Offer valid conclusions, opinions or recommendations when needed

Licensed to Berend Post berend.post@it-university.nl

Be created in timely manner.

The following were incorrect answers:

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability.

Reporting -The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 367 and 368

Question 415

Inherent risk ratings are determined by assessing the impact and likelihood of a threat or vulnerability occurring:

- ☒ after internal controls are taken into account.
- ☐ before the risk appetite is established.
- ☐ after compensating controls have been applied.
- ☐ before internal controls are taken into account.

Question 416

Which of the following is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Critical path methodology
- ☒ Time box management

Explanation:

Time box management is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources. There is a need to balance software quality and meet the delivery requirements within the

Licensed to Berend Post berend.post@it-university.nl

time box or timeframe. The project manager has some degree of flexibility and uses discretion is scoping the requirement. Timebox management can be used to accomplish prototyping or RAPID application development type in which key feature are to be delivered in a short period of time.

The following were incorrect answers:

Critical path Method -The critical path method (CPM) is an algorithm for scheduling a set of project activities

Gantt Chart -A Gantt chart is a type of bar chart, developed by Henry Gantt in the 1910s, that illustrates a project schedule. Gantt charts illustrate the start and finish dates of the terminal elements and summary elements of a project. Terminal elements and summary elements comprise the work breakdown structure of the project. Modern Gantt charts also show the dependency (i.e. precedence network) relationships between activities. Gantt charts can be used to show current schedule status using percent-complete shadings and a vertical "TODAY" line as shown here.

Functional Point Analysis -Function Point Analysis (FPA) is an ISO recognized method to measure the functional size of an information system. The functional size reflects the amount of functionality that is relevant to and recognized by the user in the business. It is independent of the technology used to implement the system.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 154

Question 417

An IS auditor is reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents. Which of the following observations should be of MOST concern to the auditor?

☐ Training was not provided to the department that handles intellectual property and patents.
☐ Logging and monitoring for content filtering is not enabled.
☐ The collaboration tool is hosted and can only be accessed via an Internet browser.
☒ Employees can share files with users outside the company through collaboration tools.

Licensed to Berend Post berend.post@it-university.nl

Question 418

Which of the following is the MOST effective way to assess whether an outsourcer's controls are following the service level agreement (SLA)?

- ☒ Perform an onsite review of the outsourcer.
- ☐ Review the outsourcer's monthly service reports.
- ☐ Perform a review of penalty clauses for non-performance.
- ☐ Review an internal audit report from the outsourcer's auditor.

Question 419

During the procurement process, which of the following would be the BEST indication that prospective vendors will meet the organization's needs?

- ☐ An account transition manager has been identified.
- ☒ Expected service levels are defined.
- ☐ The vendor's subcontractors have been identified.
- ☐ The service catalog is documented.

Question 420

Which of the following ensures confidentiality of information sent over the internet?

- ☐ Digital signature
- ☐ Digital certificate
- ☐ Online Certificate Status Protocol
- ☒ Private key cryptosystem

Explanation:

Explanation:

Confidentiality is assured by a private key cryptosystem. Digital signatures assure data integrity, authentication and nonrepudiation, but not confidentially. A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity; therefore, it does not address confidentiality. Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate.

Licensed to Berend Post berend.post@it-university.nl

Question 421

When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

- ☒ There could be a question regarding the legal jurisdiction.
- ☐ Having a provider abroad will cause excessive costs in future audits.
- ☐ The auditing process will be difficult because of the distance.
- ☐ There could be different auditing norms.

Explanation:

Explanation:

In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

Question 422

Which of the following type of a computer network is a WAN that are limited to a city?

- ☐ LAN
- ☒ MAN
- ☐ SAN
- ☐ PAN

Explanation:

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN.

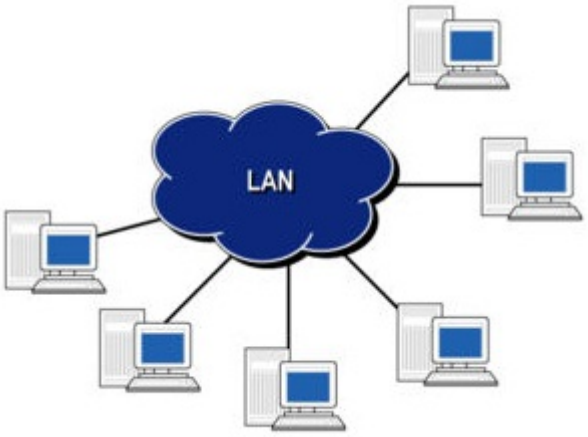
For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

Local Area Network

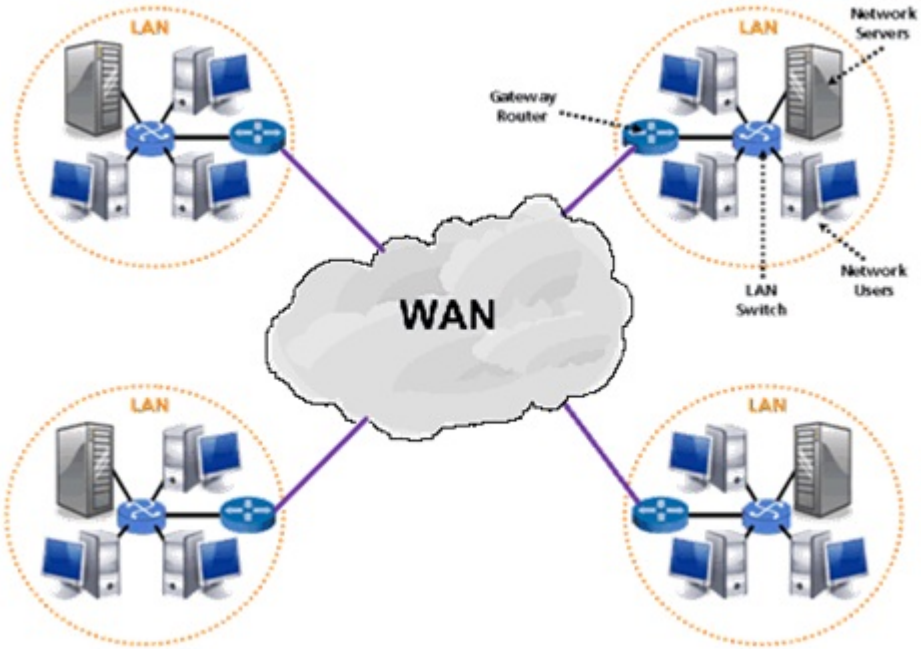
Licensed to Berend Post berend.post@it-university.nl



Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Wide Area Network



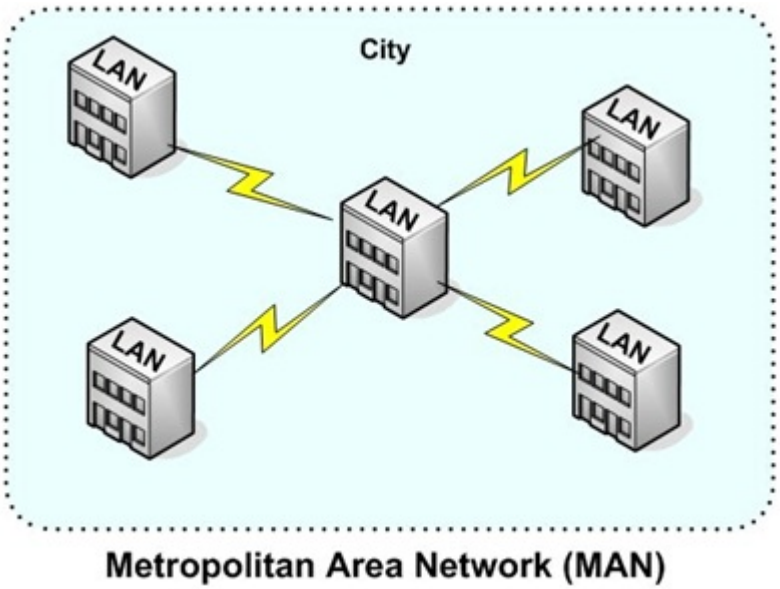
Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are

Licensed to Berend Post berend.post@it-university.nl

determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

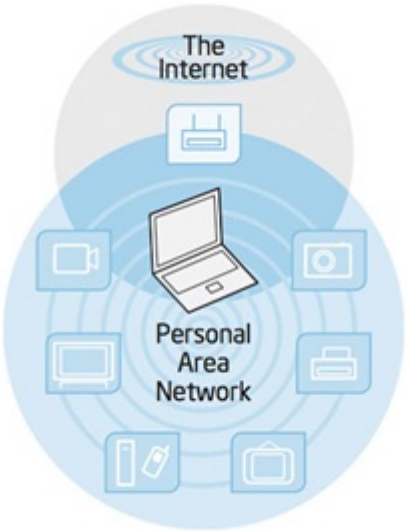


Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network

Licensed to Berend Post berend.post@it-university.nl



Storage Area Network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

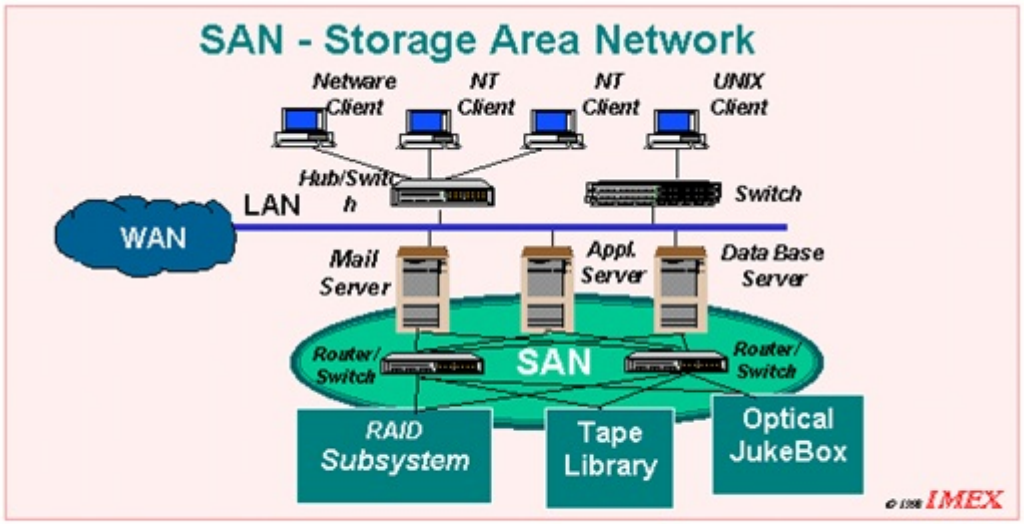


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for

Licensed to Berend Post berend.post@it-university.nl

communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Question 423

Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

- ☒ Unauthorized access from outside the organization
- ☐ Unauthorized access from within the organization
- ☐ A delay in Internet connectivity
- ☐ A delay in downloading using File Transfer Protocol (FTP)

Explanation:

Explanation:

Firewalls are meant to prevent outsiders from gaining access to an organization's computer systems through the internet gateway. They form a barrier with the outside world, but are not intended to address access by internal users; they are more likely to cause delays than address such concerns.

Licensed to Berend Post berend.post@it-university.nl

Question 424

As part of an IS audit, the auditor notes the practices listed below. Which of the following would be a segregation of duties concern?

- ☐ Operators are degaussing magnetic tapes during night shifts.
- ☐ System programmers have logged access to operating system parameters.
- ☐ System programmers are performing the duties of operators.
- ☒ Operators are acting as tape librarians on alternate shifts.

Question 425

An organization has replaced all of the storage devices at its primary data center with new, higher capacity units. The replaced devices have been installed at the disaster recovery site to replace older units. An IS auditor's PRIMARY concern would be whether:

- ☒ the procurement was in accordance with corporate policies and procedures
- ☐ the relocation plan has been communicated to all concerned parties
- ☐ a hardware maintenance contract is in place for both old and new storage devices
- ☐ the recovery site devices can handle the storage requirements

Question 426

Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

- ☐ poorer performance.
- ☐ poor scalability.
- ☐ weak infrastructure.
- ☒ high costs in terms of training and maintenance.
- ☐ None of the choices.

Explanation:

Explanation:

An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.

Licensed to Berend Post berend.post@it-university.nl

Question 427

Which of the following should an IS auditor expect to find in an organization's information security policies?

- ☐ Authentication requirements
- ☐ Asset provisioning lifecycle
- ☐ Security configuration settings
- ☒ Secure coding procedures

Question 428

Who is primarily responsible for storing and safeguarding the data?

- ☐ Data Owner
- ☐ Data User
- ☒ Data Steward
- ☐ Security Administrator

Explanation:

Data Steward or data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

For CISA exam you should know below roles in an organization

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Data Owner- These peoples are generally managers and directors responsible for using information for running and controlling the business.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Security Administrator - Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number361

Question 429

An employee who denies accusations of sending inappropriate images to other employees has been discharged. For evidential purposes, the mail database for the discharged employee's computer should be:

- ☐ deleted as it could subject the organization to further legal liability
- ☐ impounded by physically removing the disk drive
- ☒ backed up to the server, where its access can be tightly restricted
- ☐ copied to write-once, read-many media using the computer's OS tools

Question 430

Which of the following controls would BEST ensure that payroll system rate changes are valid?

- ☐ Only a payroll department manager can input the new rate.
- ☐ Rate changes require visual verification before acceptance.
- ☐ Rate changes must be entered twice to ensure that they are entered correctly.
- ☒ Rate changes are reported to and independently verified by a manager.

Question 431

Which of the following is a PRIMARY security responsibility of an information owner?

- ☐ Determining the controls associated with information classification
- ☐ Testing information classification controls
- ☒ Maintaining the integrity of data in the information systems
- ☐ Deciding what level of classification the information requires

Licensed to Berend Post berend.post@it-university.nl

Question 432

An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's BEST recommendation would be to:

- ☐ recruit more monitoring personnel.
- ☐ fine tune the intrusion detection system (IDS).
- ☐ reduce the firewall rules.
- ☒ establish criteria for reviewing alerts.

Question 433

The independence of an IS auditor auditing an application is maintained if the auditor's role is limited to:

- ☐ creating system specifications.
- ☒ defining user requirements.
- ☐ recommending system enhancements.
- ☐ designing access control rules.

Question 434

Which of the following is the BEST reason to perform root cause analysis after a critical server failure?

- ☒ To enable appropriate corrective measures
- ☐ To enable the gathering of system availability data
- ☐ To enable timely follow-up audits
- ☐ To enable the optimization of IT investments

Question 435

An IS auditor is reviewing the process followed in identifying and prioritizing the critical business processes. This process is part of the:

- ☐ balanced scorecard.
- ☐ business impact analysis (BIA).
- ☒ operations component of the business continuity plan (BCP).
- ☐ enterprise risk management plan.

Licensed to Berend Post berend.post@it-university.nl

Question 436

Which of the following attack best describe “Computer is the target of a crime” and “Computer is the tool of a crime”?

- ☒ Denial of Service (DoS) and Installing Key loggers
- ☐ War Driving and War Chalking
- ☐ Piggybacking and Race Condition
- ☐ Traffic analysis and Eavesdropping

Explanation:

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. (See botnet) DoS (Denial of Service) attacks are sent by one person or system.

Keystroke logging, often referred to as key logging or keyboard capturing, is the action of recording (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It also has very legitimate uses in studies of human-computer interaction. There are numerous key logging methods, ranging from hardware and software-based approaches to acoustic analysis.

There are four types of a computer crimes:

1. Computer is the target of a crime – Perpetrator uses another computer to launch an attack. In this attack the target is a specific identified computer. Ex. Denial of Service (DoS), hacking

2. Computer is the Subject of a crime – In this attack perpetrator uses computer to commit crime and the target is another computer. In this attack, target may or may not be defined. Perpetrator launches attack with no specific target in mind. Ex. Distributed DoS, Malware

3. Computer is the tool of a crime – Perpetrator uses computer to commit crime but the target is not a computer. Target is the data or information stored on a computer. Ex. Fraud, unauthorized access, phishing, installing key logger

4. Computer Symbolizes Crime – Perpetrator lures the user of a computer to get confidential information. Target is user of computer. Ex. Social engineering methods like Phishing, Fake website, Scam Mails, etc

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they’ve gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

The following reference(s) were/was used to create this question:

CISA review Manual 2014. Page number 321

http://en.wikipedia.org/wiki/Denial-of-service_attack

http://en.wikipedia.org/wiki/Eavesdropping

http://en.wikipedia.org/wiki/Traffic_analysis

http://www.techopedia.com/definition/4020/masquerade-attack

Licensed to Berend Post berend.post@it-university.nl

Question 437

An IS auditor is reviewing an organization's sales and purchasing system due to ongoing data quality issues. An analysis of which of the following would provide the MOST useful information to determine the revenue loss?

- ☐ Correlation between the number of issues and average downtime
- ☐ Cost of implementing data validation controls within the system
- ☐ Comparison of the cost of data acquisition and loss in sales revenue
- ☒ Correlation between data errors and loss in value of transactions

Question 438

Which of the following is the BEST way to evaluate the effectiveness of access controls to an internal network?

- ☒ Perform a system penetration test
- ☐ Test compliance with operating procedures
- ☐ Review access rights
- ☐ Review router configuration tables

Question 439

An organization plans to receive an automated data feed into its enterprise data warehouse from a third-party service provider. Which of the following would be the BEST way to prevent accepting bad data?

- ☐ Appoint data quality champions across the organization
- ☐ Obtain error codes indicating failed data feeds
- ☐ Purchase data cleansing tools from a reputable vendor
- ☒ Implement business rules to reject invalid data

Question 440

ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?

- ☐ Reliability
- ☐ Usability
- ☒ Functionality
- ☐ Maintainability

Explanation:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties.

Licensed to Berend Post berend.post@it-university.nl

The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

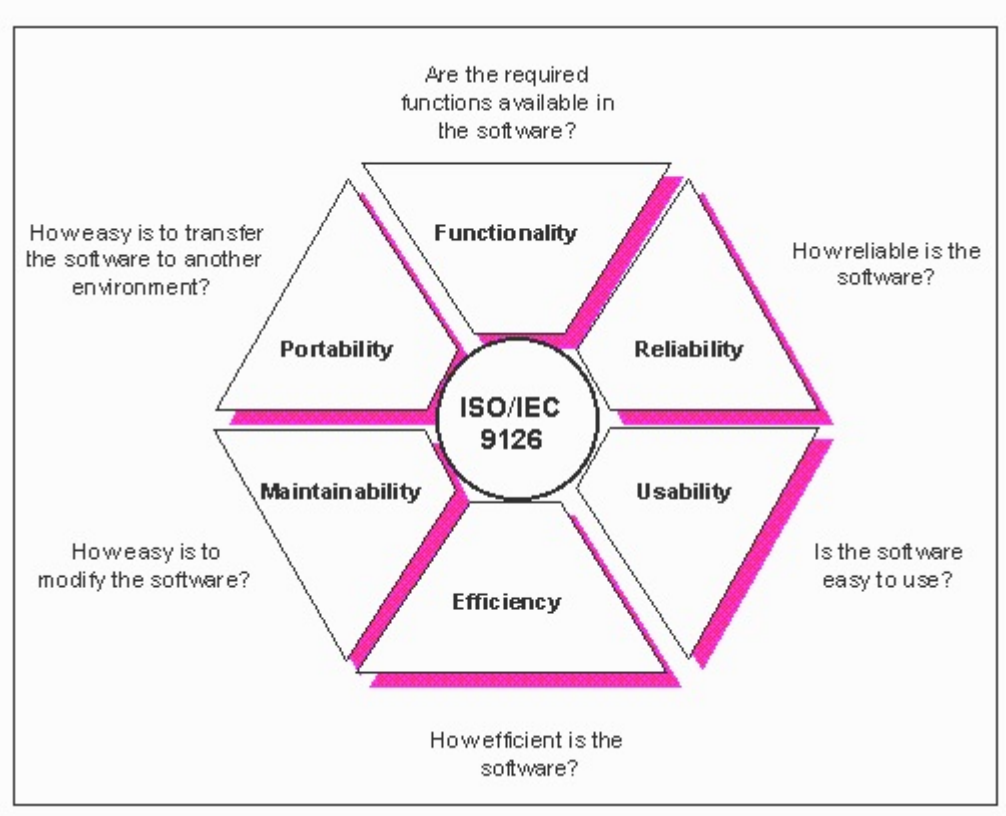
Functionality Compliance

For CISA Exam you should know below information about ISO 9126 model:

ISO/IEC 9126 Software engineering — Product quality was an international standard for the evaluation of software quality. It has been replaced by ISO/IEC 25010:2011.[1] The fundamental objective of the ISO/IEC 9126 standard is to address some of the well-known human biases that can adversely affect the delivery and perception of a software development project. These biases include changing priorities after the start of a project or not having any clear definitions of "success." By clarifying, then agreeing on the project priorities and subsequently converting abstract priorities (compliance) to measurable values (output data can be validated against schema X with zero intervention), ISO/IEC 9126 tries to develop a common understanding of the project's objectives and goals.

ISO 9126

Licensed to Berend Post berend.post@it-university.nl



The standard is divided into four parts:

Quality model

External metrics

Internal metrics

Quality in use metrics.

Quality Model

The quality model presented in the first part of the standard, ISO/IEC 9126-1,[2] classifies software quality in a structured set of characteristics and sub-characteristics as follows:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

Functionality Compliance

Licensed to Berend Post berend.post@it-university.nl

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Maturity

Fault Tolerance

Recoverability

Reliability Compliance

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

Understandability

Learn ability

Operability

Attractiveness

Usability Compliance

Efficiency - A set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.

Time Behavior

Resource Utilization

Efficiency Compliance

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

Analyzability

Changeability

Stability

Testability

Maintainability Compliance

Portability - A set of attributes that bear on the ability of software to be transferred from one environment to another.

Adaptability

Install ability

Licensed to Berend Post berend.post@it-university.nl

Co-Existence

Replace ability

Portability Compliance

Each quality sub-characteristic (e.g. adaptability) is further divided into attributes. An attribute is an entity which can be verified or measured in the software product. Attributes are not defined in the standard, as they vary between different software products.

Software product is defined in a broad sense: it encompasses executables, source code, architecture descriptions, and so on. As a result, the notion of user extends to operators as well as to programmers, which are users of components such as software libraries.

The standard provides a framework for organizations to define a quality model for a software product. On doing so, however, it leaves up to each organization the task of specifying precisely its own model. This may be done, for example, by specifying target values for quality metrics which evaluates the degree of presence of quality attributes.

Internal Metrics

Internal metrics are those which do not rely on software execution (static measure)

External Metrics

External metrics are applicable to running software.

Quality in Use Metrics

Quality in use metrics are only available when the final product is used in real conditions.

Ideally, the internal quality determines the external quality and external quality determines quality in use.

This standard stems from the GE model for describing software quality, presented in 1977 by McCall et al., which is organized around three types of Quality Characteristics:

Factors (To specify): They describe the external view of the software, as viewed by the users.

Criteria (To build): They describe the internal view of the software, as seen by the developer.

Metrics (To control): They are defined and used to provide a scale and method for measurement.

 Licensed to Berend Post berend.post@it-university.nl

ISO/IEC 9126 distinguishes between a defect and a nonconformity, a defect being The nonfulfillment of intended usage requirements, whereas a nonconformity is The nonfulfillment of specified requirements. A similar distinction is made between validation and verification, known as V&V in the testing trade.

The following were incorrect answers:

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 441

What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program?

- ☐ Network-monitoring software
- ☒ A system downtime log
- ☐ Administration activity reports
- ☐ Help-desk utilization trend reports

Explanation:

Explanation:

A system downtime log can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program.

Licensed to Berend Post berend.post@it-university.nl

Question 442

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- ☐ Define a balanced scorecard (BSC) for measuring performance
- ☐ Consider user satisfaction in the key performance indicators (KPIs)
- ☒ Select projects according to business benefits and risks
- ☐ Modify the yearly process of defining the project portfolio

Explanation:

Explanation:

Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

Question 443

When reviewing capacity monitoring, an IS auditor notices several incidents where storage capacity limits were reached, while the average utilization was below 30%. Which of the following would the IS auditor MOST likely identify as the root cause?

- ☐ The IT response to the alerts was too slow.
- ☐ The amount of data produced was unacceptable for operations.
- ☐ The storage space should have been enlarged in time.
- ☒ The dynamics of the utilization were not properly taken into account.

Question 444

Which of the following is the MOST effective mitigation strategy to protect confidential information from insider threats?

- ☐ Implementing authentication mechanisms
- ☐ Performing an entitlement review process
- ☐ Defining segregation of duties
- ☒ Establishing authorization controls.

Licensed to Berend Post berend.post@it-university.nl

Question 445

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- ☐ digest signature.
- ☐ electronic signature.
- ☒ digital signature.
- ☐ hash signature.

Explanation:

Explanation:

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

Question 446

An IT department has given a vendor remote access to the internal network for troubleshooting network performance problems. After discovering the remote activity during a firewall log review, which of the following is the BEST course of action for an information security manager?

- ☐ Revoke the access.
- ☐ Review the related service level agreement (SLA).
- ☒ Determine the level of access granted.
- ☐ Declare a security incident.

Question 447

An organization has established three IT processing environments: development, test, and production. The MAJOR reason for separating the development and test environments is to:

- ☐ obtain segregation of duties between IT staff and end users.
- ☐ limit the users' access rights to the test environment.
- ☒ perform testing in a stable environment.
- ☐ protect the programs under development from unauthorized testing.

Licensed to Berend Post berend.post@it-university.nl

Question 448

An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

- ☒ matching control totals of the imported data to control totals of the original data.
- ☐ sorting the data to confirm whether the data are in the same order as the original data.
- ☐ reviewing the printout of the first 100 records of original data with the first 100 records of imported data.
- ☐ filtering data for different categories and matching them to the original data.

Explanation:

Explanation:

Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported datA. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification and confirms the accuracy of only these records. Filtering data for different categories and matching them to original data would still require that control totals be developed to confirm the completeness of the data.

Question 449

How is the risk of improper file access affected upon implementing a database system?

- ☐ Risk varies.
- ☐ Risk is reduced.
- ☐ Risk is not affected.
- ☒ Risk is increased.

Explanation:

Explanation:

Improper file access becomes a greater risk when implementing a database system.

Question 450

An IS auditor has been invited to join an IT project team responsible for building and deploying a new digital customer marketing platform. Which of the following is the BEST way for the auditor to support this project while maintaining independence?

- ☒ Develop selection criteria for potential digital technology vendors.
- ☐ Conduct an industry peer benchmarking exercise and advise on alternative solutions.
- ☐ Conduct a risk assessment of the proposed initiative.
- ☐ Design controls based on current regulatory requirements for digital technologies.

Licensed to Berend Post berend.post@it-university.nl

Question 451

The information security function in a large organization is MOST effective when:

- ☒ decentralized as close to the user as possible.
- ☐ the function reports directly to the IS operations manager.
- ☐ partnered with the IS development team to determine access rights.
- ☐ established at a corporate-wide level.

Question 452

Which of the following metrics would be MOST helpful to an IS auditor in evaluating an organization's security incident response management capability?

- ☒ Number of business interruptions due to IT security incidents per year.
- ☐ Number of IT security incidents reported per month
- ☐ Number of malware infections in business applications detected per day.
- ☐ Number of alerts generated by intrusion detection systems (IDS) per minute.

Question 453

Regarding digital signature implementation, which of the following answers is correct?

- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
- ☒ A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Explanation:

Explanation:

A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

Licensed to Berend Post berend.post@it-university.nl

Question 454

In which of the following payment mode, an issuer attempts to emulate physical cash by creating digital certificates, which are purchased by users who redeem them with the issuer at a later date?

- ☒ Electronic Money Model
- ☐ Electronics Checks model
- ☐ Electronic transfer model
- ☐ Electronic withdraw model

Explanation:

In an electronic money model issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems – the issuer and the user. An issuer is an entity that operates the payment service. An issuer holds the items that the payment represents. The user of the payment service performs two main functions- making payments and receiving payments – and therefore can be described as a payer or payee receptively.

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

Electronic Withdraw Model – Not a valid type of payment system.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 183

Question 455

Which of the following roles combined with the role of a database administrator (DBA) will create a segregation of duties conflict?

- ☐ Quality assurance
- ☐ Systems analyst
- ☐ Application end user
- ☒ Security administrator

Question 456

Which of the following provides the framework for designing and developing logical access controls?

- ☒ Information systems security policy
- ☐ Access control lists
- ☐ Password management
- ☐ System configuration files

Explanation:

Explanation:

The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control

Licensed to Berend Post berend.post@it-university.nl

lists, password management and systems configuration files are tools for implementing the access controls.

Question 457

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model depict data entities and how they relate?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☒ Entity relationship diagrams

Explanation:

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Licensed to Berend Post berend.post@it-university.nl

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data

Licensed to Berend Post berend.post@it-university.nl

repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram – De-construct business processes.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 458

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

-The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
-The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.
- the plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The IS auditor's report should recommend that:

- ☐ the deputy CEO be censured for their failure to approve the plan.
- ☐ a board of senior managers is set up to review the existing plan.
- ☐ the existing plan is approved and circulated to all key management and staff.
- ☒ a manager coordinates the creation of a new or revised plan within a defined time limit.

Explanation:

Explanation:

The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend.

Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation, and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short time is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.

Licensed to Berend Post berend.post@it-university.nl

Question 459

When reviewing an organization's IT governance processes, which of the following provides the BEST indication that information security expectations are being met at all levels?

- ☒ Achievement of established security metrics
- ☐ Approval of the security program by senior management
- ☐ Utilization of an internationally recognized security standard
- ☐ Implementation of a comprehensive security awareness program

Question 460

What should IS auditors always check when auditing password files?

- ☐ That deleting password files is protected
- ☒ That password files are encrypted
- ☐ That password files are not accessible over the network
- ☐ That password files are archived

Explanation:

Explanation:

IS auditors should always check to ensure that password files are encrypted.

Question 461

Which of the following BEST ensures the integrity of a server's operating system?

- ☐ Protecting the server in a secure location
- ☐ Setting a boot password
- ☒ Hardening the server configuration
- ☐ Implementing activity logging

Explanation:

Explanation:

Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario-it is a detective control (not a preventive one), and the attacker who already gained privileged access can modify logs or disable them.

Licensed to Berend Post berend.post@it-university.nl

Question 462

Which of the following is the MOST effective data loss control when connecting a personally owned mobile device to the corporate email system?

- ☐ A senior manager must approve each new connection.
- ☐ Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
- ☒ Email must be stored in an encrypted format on the mobile device.
- ☐ Users must agree to allow the mobile device to be wiped if it is lost.

Question 463

Which of the following is the unique identifier within and IPSec packet that enables the sending host to reference the security parameter to apply?

- ☒ SPI
- ☐ SA
- ☐ ESP
- ☐ AH

Explanation:

The Security Parameter Index (SPI) is the unique identifier that enables the sending host to reference the security parameter to apply in order to decrypt the packet.

For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.

In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

Licensed to Berend Post berend.post@it-university.nl

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

SA – Security Association (SA) defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc.

ESP – Encapsulation Security Payload (ESP) is used to support authentication of sender and encryption of data

AH – Authentication Header allows authentication of a sender of a data.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 353

Question 464

In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- ☒ Nonrepudiation
- ☐ Encryption
- ☐ Authentication
- ☐ Integrity

Explanation:

Explanation:

Nonrepudiation, achieved through the use of digital signatures, prevents the claimed sender from later denying that they generated and sent the message. Encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made. Authentication is necessary to establish the identification of all parties to a communication. Integrity ensures that transactions are accurate but does not provide the identification of the customer.

Licensed to Berend Post berend.post@it-university.nl

Question 465

An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

- ☐ Developer access to production
- ☐ Lack of system integrity
- ☐ Outdated system documentation
- ☒ Loss of application support

Question 466

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- ☒ improve internal control procedures.
- ☐ harden the network to industry best practices.
- ☐ highlight the importance of incident response management to management.
- ☐ improve employee awareness of the incident response process.

Explanation:

Explanation:

A postincident review examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls. Understanding the purpose and structure of postincident reviews and follow-up procedures enables the information security manager to continuously improve the security program. Improving the incident response plan based on the incident review is an internal (corrective) control. The network may already be hardened to industry best practices. Additionally, the network may not be the source of the incident. The primary objective is to improve internal control procedures, not to highlight the importance of incident response management (IRM), and an incident response (IR) review does not improve employee awareness.

Question 467

Which of the following is a good tool to use to help enforcing the deployment of good passwords?

- ☒ password cracker
- ☐ local DoS attacker
- ☐ network hacker
- ☐ remote windowing tool
- ☐ None of the choices.

Explanation:

Explanation:

"Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A

Licensed to Berend Post berend.post@it-university.nl

good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters. You may want to run a "password cracker" program periodically, and require users to immediately change any easily cracked passwords. In any case ask them to change their passwords every 90 to 120 days."

Question 468

Which of the following is a prerequisite to help ensure that IS hardware and software support the delivery of mission-critical functions?

- ☐ Control over IS infrastructure expenditure
- ☐ An independent audit of the process
- ☒ A comprehensive IS applications architecture
- ☐ Documented emergency change procedures

Question 469

Which of the following is MOST important to consider when developing a disaster recovery plan?

- ☐ Business continuity plan (BCP)
- ☐ Feasibility assessment
- ☒ Business impact analysis (BIA)
- ☐ Cost-benefit analysis

Question 470

An IS auditor is reviewing database log settings and notices that only INSERT and DELETE operations are being monitored in the database. What is the MOST significant risk?

- ☐ Metadata may not be logged
- ☒ Newly added records may not be logged
- ☐ Purged records may not be logged
- ☐ Changes to existing records may not be logged

Question 471

Which of the following methodologies is MOST appropriate to use for developing software with incomplete requirements?

- ☐ Process-based
- ☐ Critical chain
- ☐ Waterfall
- ☒ Agile

Licensed to Berend Post berend.post@it-university.nl

Question 472

In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

- ☐ Automated logging of changes to development libraries
- ☐ Additional staff to provide separation of duties
- ☒ Procedures that verify that only approved program changes are implemented
- ☐ Access controls to prevent the operator from making program modifications

Explanation:

Explanation:

While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process.

Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

Question 473

One major improvement in WPA over WEP is the use of a protocol which dynamically changes keys as the system is used. What protocol is this?

- ☐ SKIP
- ☐ RKIP
- ☐ OKIP
- ☐ EKIP
- ☒ TKIP
- ☐ None of the choices.

Explanation:

Explanation:

Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used.

Licensed to Berend Post berend.post@it-university.nl

Question 474

An IS auditor discovers that validation controls in a web application have been moved from the server side into the browser to boost performance. This would MOST likely increase the risk of a successful attack by:

- ☐ phishing
- ☒ structured query language (SQL) injection
- ☐ denial of service (DoS)
- ☐ buffer overflow

Question 475

Which of the following is by far the most common prevention system from a network security perspective?

- ☒ Firewall
- ☐ IDS
- ☐ IPS
- ☐ Hardened OS
- ☐ Tripwire
- ☐ None of the choices.

Explanation:

Explanation:

User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

Question 476

Which of the following would be MOST useful when analyzing computer performance?

- ☐ Report of off-peak utilization and response time
- ☒ Tuning of system software to optimize resource usage
- ☐ Operations report of user dissatisfaction with response time
- ☐ Statistical metrics measuring capacity utilization

Licensed to Berend Post berend.post@it-university.nl

Question 477

Which of the following is an attribute of the control self-assessment (CSA) approach?

- ☒ Broad stakeholder involvement
- ☐ Auditors are the primary control analysts
- ☐ Limited employee participation
- ☐ Policy driven

Explanation:

Explanation:

The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, at! of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

Question 478

Which of the following data validation edits is effective in detecting transposition and transcription errors?

- ☐ Range check
- ☒ Check digit
- ☐ Validity check
- ☐ Duplicate check

Explanation:

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteria. In a duplicate check, newer fresh transactions are matched to those previously entered to ensure that they are not already in the system.

Question 479

Which of the following are valid examples of Malware:

- ☐ viruses
- ☐ worms
- ☐ trojan horses
- ☐ spyware
- ☒ All of the above

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Software is considered malware based on the intent of the creator rather than any particular features. It includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted software.

Question 480

Which of the following is the MOST important advantage of participating in beta testing of software products?

- ☐ It improves vendor support and training.
- ☒ It enables an organization to gain familiarity with new products and their functionality.
- ☐ It increases an organization’s ability to retain staff who prefer to work with new technology.
- ☐ It enhances security and confidentiality.

Question 481

Which of the following provides the MOST helpful information to determine how much data an organization can afford to lose when a critical system failure occurs?

- ☐ Industry data loss statistics
- ☐ Risk assessment results
- ☒ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)

Question 482

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

- ☐ Identifying relevant roles for an enterprise IT governance framework
- ☒ Verifying that legal, regulatory and contractual requirements are being met
- ☐ Making decisions regarding risk response and monitoring of residual risk
- ☐ Providing independent and objective feedback to facilitate improvement of IT processes

Licensed to Berend Post berend.post@it-university.nl

Question 483

Which of the following is the PRIMARY objective of implementing IT governance?

- ☐ Resource management
- ☒ Performance measurement
- ☐ Value delivery
- ☐ Strategic planning

Question 484

A contract bid is digitally signed and electronically mailed. The PRIMARY advantage to using a digital signature is that:

- ☐ the bid cannot be forged even if the keys are compromised.
- ☐ the bid and the signature can be copied from one document to another.
- ☒ the signature can be authenticated even if no encryption is used.
- ☐ any alteration of the bid will invalidate the signature.

Question 485

Which of the following is the BEST way to improve the timely reporting of information security incidents?

- ☐ Perform periodic simulations with the incident response team.
- ☐ Incorporate security procedures in help desk processes.
- ☐ Integrate an intrusion detection system (IDS) in the DMZ.
- ☒ Regularly reassess and update the incident response plan.

Question 486

Which of the following is MOST important to include in a contract with a critical service provider to help ensure alignment with the organization's information security program?

- ☐ Escalation paths
- ☐ Right-to-audit clause
- ☐ Termination language
- ☒ Key performance indicators (KPIs)

Licensed to Berend Post berend.post@it-university.nl

Question 487

Which of the following layer of an enterprise data flow architecture is concerned with transporting information between the various layers?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☒ Application messaging layer
- ☐ Data access layer

Explanation:

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Licensed to Berend Post berend.post@it-university.nl

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Licensed to Berend Post berend.post@it-university.nl

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Licensed to Berend Post berend.post@it-university.nl

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are

organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 488

During what process should router access control lists be reviewed?

- ☐ Environmental review
- ☒ Network security review
- ☐ Business continuity review
- ☐ Data integrity review

Explanation:

Explanation:

Network security reviews include reviewing router access control lists, port scanning, internal and external connections to the system, etc. Environmental reviews, business continuity reviews and data integrity reviews do not require a review of the router access control lists.

Question 489

An IS auditor has completed an audit of an organization's accounts payable system. Which of the following should be rated as the HIGHEST risk in the audit report and requires immediate remediation?

- ☒ Lack of segregation of duty controls for reconciliation of payment transactions
- ☐ Lack of segregation of duty controls for removal of vendor records
- ☐ Lack of segregation of duty controls for updating the vendor master file
- ☐ Lack of segregation of duty controls for reversing payment transactions

Licensed to Berend Post berend.post@it-university.nl

Question 490

An IS auditor discovers a recurring software control process issue that severely impacts the efficiency of a critical business process. Which of the following is the BEST recommendation?

- ☐ Replace the malfunctioning system.
- ☐ Determine the compensating controls.
- ☐ Identify other impacted processes.
- ☒ Determine the root cause of the issue.

Question 491

Digital signatures are an effective control method for information exchange over an insecure network because they:

- ☒ enable nonrepudiation.
- ☐ are under the sole custody of the receiver.
- ☐ are constant over time.
- ☐ authenticate the user biometrically.

Question 492

A development team has designed a new application and incorporated best practices for secure coding. Prior to launch, which of the following is the IS auditor's BEST recommendation to mitigate the associated security risk?

- ☒ User acceptance testing
- ☐ Unit testing
- ☐ Integration testing
- ☐ Penetration testing

Question 493

Who is responsible for restricting and monitoring access of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☒ Security Administrator

Explanation:

Security administrator are responsible for providing adequate and logical security for IS programs, data and equipment.

For CISA exam you should know below roles in an organization

Licensed to Berend Post berend.post@it-university.nl

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator-Security administrator are responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Data Owner - These peoples are generally managers and directors responsible for using information for running and controlling the business.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 361

Question 494

To BEST evaluate the effectiveness of a disaster recovery plan, the IS auditor should review the:

- ☒ test plan and results of past tests.
- ☐ plans and procedures in the business continuity plan.
- ☐ capacity of backup facilities.
- ☐ hardware and software inventory.

Licensed to Berend Post berend.post@it-university.nl

Question 495

Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

- ☒ Simple Network Management Protocol
- ☐ File Transfer Protocol
- ☐ Simple Mail Transfer Protocol
- ☐ Telnet

Explanation:

Explanation:

The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

Question 496

The MOST important success factor in planning a penetration test is:

- ☐ the documentation of the planned testing procedure.
- ☐ scheduling and deciding on the timed length of the test.
- ☒ the involvement of the management of the client organization.
- ☐ the qualifications and experience of staff involved in the test.

Explanation:

Explanation:

The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

Question 497

A reduction in which of the following would indicate improved performance in the administration of information security?

- ☐ IT security awareness training days
- ☐ Number of staff involved in security administration
- ☒ Systems subject to an intrusion detection process
- ☐ Turnaround time for requests for new user access

Licensed to Berend Post berend.post@it-university.nl

Question 498

An IS auditor is reviewing an organization's incident management processes and procedures. Which of the following observations should be the auditor's GREATEST concern?

- ☐ Ineffective incident classification
- ☐ Ineffective incident prioritization
- ☒ Ineffective incident detection
- ☐ Ineffective post-incident review

Question 499

Adopting a service-oriented architecture would MOST likely:

- ☐ inhibit integration with legacy systems.
- ☐ compromise application software security.
- ☒ facilitate connectivity between partners.
- ☐ streamline all internal processes.

Question 500

Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

- ☐ Server antivirus software
- ☒ Virus walls
- ☐ Workstation antivirus software
- ☐ Virus signature updating

Explanation:

Explanation:

An important means of controlling the spread of viruses is to detect the virus at the point of entry, before it has an opportunity to cause damage. In an interconnected corporate network, virus scanning software, used as an integral part of firewall technologies, is referred to as a virus wall. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. The presence of virus walls does not preclude the necessity for installing virus detection software on servers and workstations within the network, but network- level protection is most effective the earlier the virus is detected. Virus signature updating is a must in all circumstances, networked or not.

Licensed to Berend Post berend.post@it-university.nl

Question 501

Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

- ☐ Attribute sampling
- ☒ Generalized audit software (GAS)
- ☐ Test data
- ☐ Integrated test facility (ITF)

Explanation:

Explanation:

Generalized audit software (GAS) would enable the auditor to review the entire invoice file to look for those items that meet the selection criteria. Attribute sampling would aid in identifying records meeting specific conditions, but would not compare one record to another to identify duplicates. To detect duplicate invoice records, the IS auditor should check all of the items that meet the criteria and not just a sample of the items. Test data are used to verify program processing, but will not identify duplicate records. An integrated test facility (ITF) allows the IS auditor to test transactions through the production system, but would not compare records to identify duplicates.

Question 502

Diskless workstation is an example of:

- ☐ Handheld devices
- ☒ Thin client computer
- ☐ Personal computer
- ☐ Midrange server

Explanation:

Diskless workstations are example of Thin client computer.

A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex

Licensed to Berend Post berend.post@it-university.nl

scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers

A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers

Licensed to Berend Post berend.post@it-university.nl

A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1] They are also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a mice (microphone) pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as ultra-books or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Smartphone, tablets and other handheld devices

A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard.

A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers. Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Thin Client computers

A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

The other types of computers are not example of diskless workstation.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 246

http://en.wikipedia.org/wiki/Thin_client

http://en.wikipedia.org/wiki/Mobile_device

http://en.wikipedia.org/wiki/Personal_computer

http://en.wikipedia.org/wiki/Classes_of_computers

http://en.wikipedia.org/wiki/Laptop

Question 503

An IS auditor is evaluating a virtual server environment and learns that the production server, development server, and management console are housed in the same physical host. What should be the auditor's PRIMARY concern?

- ☒ The physical host is a single point of failure
- ☐ The management console is a single point of failure
- ☐ The development server and management console share the same host
- ☐ The development and production servers share the same host

Question 504

An IS auditor is analyzing a sample of accesses recorded on the system log of an application. The auditor intends to launch an intensive investigation if one exception is found. Which sampling method would be appropriate?

- ☒ Discovery sampling
- ☐ Variable sampling
- ☐ Stratified sampling
- ☐ Judgmental sampling

Licensed to Berend Post berend.post@it-university.nl

Question 505

An IS auditor is performing an audit of a large organization's operating system maintenance procedures. Which of the following findings presents the GREATEST risk?

- ☐ Some internal servers cannot be patched due to software incompatibility.
- ☐ The configuration management database is not up-to-date.
- ☒ Vulnerability testing is not performed on the development servers.
- ☐ Critical patches are applied immediately while others follow quarterly release cycles.

Question 506

Which of the following is a key success factor for implementing IT governance?

- ☐ Embedding quality assurance processes
- ☐ Establishing an IT governance committee
- ☒ Aligning IT and business strategies
- ☐ Delivering IT projects within budget

Question 507

An IS auditor reviewing a new application for compliance with information privacy principles should be the MOST concerned with:

- ☐ nonrepudiation
- ☒ collection limitation
- ☐ availability
- ☐ awareness

Question 508

An organization is using a single account shared by personnel for its social networking marketing page. Which of the following is the BEST method to maintain accountability over the account?

- ☐ Reviewing access rights on a periodic basis
- ☐ Integrating the account with a single sign-on
- ☐ Regular monitoring of proxy server logs
- ☒ Implementing an account password check-out process

Licensed to Berend Post berend.post@it-university.nl

Question 509

Which of the following is MOST important for the IS auditor to verify when reviewing the development process of a security policy?

- ☐ Evidence of active involvement of key stakeholders
- ☐ Output from the enterprise's risk management system
- ☐ Identification of the control framework
- ☒ Evidence of management approval

Question 510

An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

- ☐ Run a low-level data wipe utility on all hard drives
- ☐ Erase all data file directories
- ☐ Format all hard drives
- ☒ Physical destruction of the hard drive

Explanation:

Explanation:

The most effective method is physical destruction. Running a low-level data wipe utility may leave some residual data that could be recovered; erasing data directories and formatting hard drives are easily reversed, exposing all data on the drive to unauthorized individuals.

Question 511

Following an IS audit, which of the following types of risk would be MOST critical to communicate to key stakeholders?

- ☐ Control
- ☐ Residual
- ☒ Audit
- ☐ Inherent

Question 512

Which of the following would BEST ensure the confidentiality of sensitive data during transmission?

- ☐ Restricting the recipient through destination IP addresses
- ☐ Sending data over public networks using Secure Sockets Layer (SSL)
- ☒ Password protecting data over virtual local area networks (VLAN)
- ☐ Sending data through proxy servers

Licensed to Berend Post berend.post@it-university.nl

Question 513

An IS auditor determines that a business continuity plan has not been reviewed and approved by management. Which of the following is the MOST significant risk associated with this situation?

- ☐ Continuity planning may be subject to resource constraints.
- ☐ The plan may not be aligned with industry best practice.
- ☐ Critical business processes may not be addressed adequately.
- ☒ The plan has not been reviewed by risk management.

Question 514

Following an IS audit recommendation, all Telnet and File Transfer Protocol (FTP) connections have been replaced by Secure Socket Shell (SSH) and Secure File Transfer Protocol (SFTP). Which risk treatment approach has the organization adopted?

- ☐ Acceptance
- ☒ Mitigation
- ☐ Avoidance
- ☐ Transfer

Question 515

Which of the following is the MOST effective type of antivirus software?

- ☐ Scanners
- ☐ Active monitors
- ☒ integrity checkers
- ☐ Vaccines

Explanation:

Explanation:

Integrity checkers compute a binary number on a known virus-free program that is then stored in a database file. This number is called a cyclical redundancy check (CRC). When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred. A change in the program could mean a virus. Scanners look for sequences of bits called signatures that are typical of virus programs. They examine memory, disk boot sectors, executables and command files for bit patterns that match a known virus. Therefore, scanners need to be updated periodically to remain effective. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions.

Active monitors can be misleading, because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files. Vaccines are known to be good antivirus software. However, they also need to be updated periodically to remain effective.

Licensed to Berend Post berend.post@it-university.nl

Question 516

Which of the following is the BEST method for determining the criticality of each application system in the production environment?

- ☐ interview the application programmers.
- ☐ Perform a gap analysis.
- ☐ Review the most recent application audits.
- ☒ Perform a business impact analysis.

Explanation:

Explanation:

A business impact analysis will give the impact of the loss of each application. Interviews with the application programmers will provide limited information related to the criticality of the systems. A gap analysis is only relevant to systems development and project management. The audits may not contain the required information or may not have been done recently.

Question 517

Which of the following is the MOST effective way to verify an organization's ability to continue its essential business operations after a disruption event? Analysis of:

- ☐ end-to-end recovery flow
- ☐ recovery point objectives (RPOs)
- ☐ call trees
- ☒ business impact analysis (BIA)

Question 518

Which of the following is a standard secure email protection protocol?

- ☒ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Explanation:

Secure Multipurpose Internet Mail Extension (S/MIME) is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of message's content's, including attachments.

The following were incorrect answers:

SSH –A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including password, binary files and administrative commands, transmitted between system on a network. SSH

Licensed to Berend Post berend.post@it-university.nl

is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation)

SET – SET is a protocol developed jointly by VISA and Master Card to secure payment transaction among all parties involved in credit card transactions among all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is a application-oriented protocol that uses trusted third party's encryption and digital-signature process, via PKI infrastructure of trusted third party institutions, to address confidentiality of information, integrity of data, cardholders authentication, merchant authentication and interoperability.

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352 and 353

Question 519

Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

- ☒ Validity check
- ☐ Reasonableness check
- ☐ Parity check
- ☐ Limit check

Question 520

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- ☒ Response
- ☐ Correction
- ☐ Detection
- ☐ Monitoring

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

Question 521

Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

- ☐ surf attack
- ☐ Traffic analysis
- ☒ Phishing
- ☐ Interrupt attack

Explanation:

Phishing technique include social engineering, link manipulation or web site forgery techniques.

For your exam you should know the information below:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of the your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article

Licensed to Berend Post berend.post@it-university.nl

entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

The following answers are incorrect:

Smurf Attack – Occurs when mix-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 323

Official ISC2 guide to CISSP CBK 3rd Edition Page number 493

http://en.wikipedia.org/wiki/Phishing

 Licensed to Berend Post berend.post@it-university.nl

Question 522

Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

- ☒ downtime costs.
- ☐ resumption costs.
- ☐ recovery costs.
- ☐ walkthrough costs.

Explanation:

Explanation:

Since the recovery time is longer in plan B, resumption and recovery costs can be expected to be lower. Walkthrough costs are not a part of disaster recovery. Since the management considered a higher window for recovery in plan B, downtime costs included in the plan are likely to be higher.

Question 523

Which of the following process consist of identification and selection of data from the imaged data set in computer forensics?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☒ Extraction

Explanation:

Extraction is the process of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device

Licensed to Berend Post berend.post@it-university.nl

must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.

Be able to withstand a barrage of legal security

Be unambiguous and not open to misinterpretation.

Be easily referenced

Contains all information required to explain conclusions reached

Offer valid conclusions, opinions or recommendations when needed

Be created in timely manner.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Reporting -The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 367 and 368

Question 524

Which of the following is the BEST method for converting a file into a format suitable for data analysis in a forensic investigation?

- ☐ Extraction
- ☒ Normalization
- ☐ Data acquisition
- ☐ Imaging

Question 525

The IS auditor of a power company finds that the radio link to a remote mountain site is experiencing systematic outages under specific weather conditions. The communications manager explains that increasing the radio power would require a new license and would help little. What is the MOST appropriate action by the IS auditor?

- ☐ Recommend that the site's data collection and transmission be non-interruptible.
- ☐ Review the installation license, permissions and associated costs.
- ☐ Recommend that the site's hardware be upgraded to record data during outages.
- ☒ Gather additional information to identify threats, vulnerabilities, and impact.

Licensed to Berend Post berend.post@it-university.nl

Question 526

The MOST likely explanation for the use of applets in an Internet application is that:

- ☐ it is sent over the network from the server.
- ☐ the server does not run the program and the output is not sent over the network.
- ☒ they improve the performance of the web server and network.
- ☐ it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Explanation:

Explanation:

An applet is a JAVA program that is sent over the network from the web server, through a web browser and to the client machine; the code is then run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network-over which the server and client are connected-drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

Question 527

Performance monitoring tools report that servers are significantly below their planned utilization. Which of the following would be the BEST recommendation?

- ☒ Consolidate physical servers.
- ☐ Review the capacity plan.
- ☐ Deploy load balancing.
- ☐ Reconfigure server settings.

Question 528

Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

- ☒ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Accuracy

Explanation:

Confidentiality supports the principle of “least privilege” by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis.

Licensed to Berend Post berend.post@it-university.nl

The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information.

Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.

An important measure to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information.

A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessible to an unauthorized person.

For your exam you should know the information below:

Integrity

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices.

Sample controls include management controls such as segregation of duties, approval checkpoints in the systems development life cycle, and implementation of testing practices that assist in providing information integrity. Well-formed transactions and security of the update programs provide consistent methods of applying changes to systems. Limiting update access to those individuals with a need to access limits the exposure to intentional and unintentional modification.

Availability

Availability is the principle that ensures that information is available and accessible to users when needed.

The two primary areas affecting the availability of systems are:

Licensed to Berend Post berend.post@it-university.nl

1. Denial-of-Service attacks and

2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

In either case, the end user does not have access to information needed to conduct business. The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes. The lack of appropriate security controls can increase the risk of viruses, destruction of data, external penetrations, or denial-of-service (DOS) attacks. Such events can prevent the system from being used by normal users.

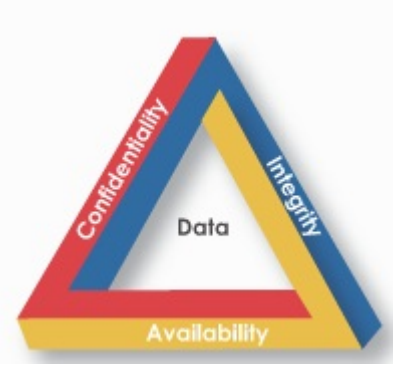
CIA

The following answers are incorrect:

Integrity- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Availability - Availability is the principle that ensures that information is available and accessible to users when needed.

Accuracy – Accuracy is not a valid CIA attribute.



Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 314

Official ISC2 guide to CISSP CBK 3rd Edition Page number 350

Licensed to Berend Post berend.post@it-university.nl

Question 529

Which of the following transmission media uses a transponder to send information?

- ☐ Copper cable
- ☐ Fiber Optics
- ☒ Satellite Radio Link
- ☐ Coaxial cable

Explanation:

Satellite radio link uses transponder to send information and are easy to intercept.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Licensed to Berend Post berend.post@it-university.nl

Coaxial Cable

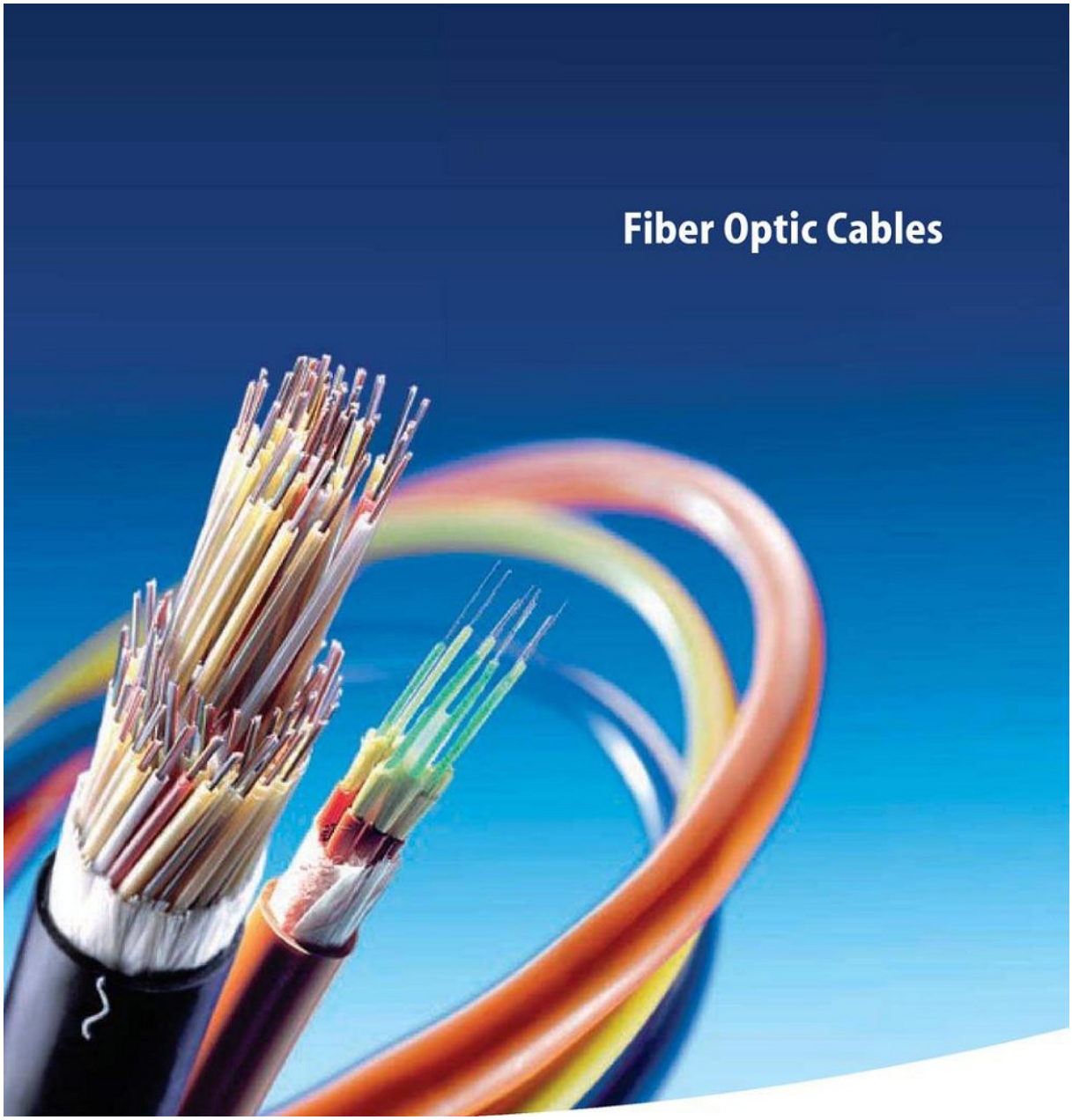
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

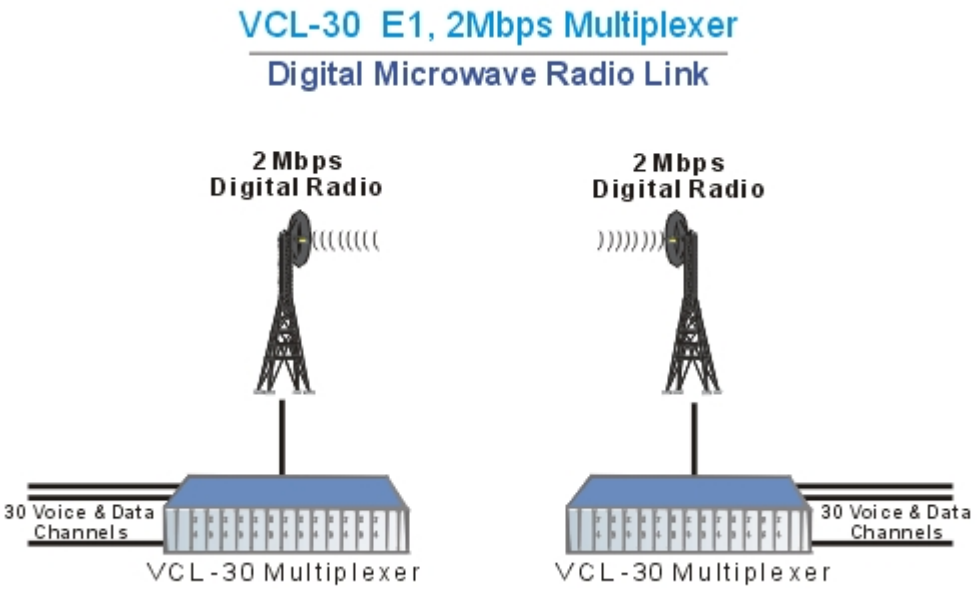
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Licensed to Berend Post berend.post@it-university.nl

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike

Licensed to Berend Post berend.post@it-university.nl

an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

Question 530

What type of risk is associated with authorized program exits (trap doors)?

- ☐ Business risk
- ☐ Audit risk
- ☐ Detective risk
- ☒ Inherent risk

Explanation:

Explanation:

Inherent risk is associated with authorized program exits (trap doors).

Question 531

An organization developed a comprehensive three-year IT strategic plan. Halfway into the plan, a major legislative change impacting the organization is enacted. Which of the following should be management's NEXTcourse of action?

- ☐ Develop specific procedural documentation related to the changed legislation.
- ☒ Assess the legislation to determine whether are required to the strategic IT plan.
- ☐ Perform a risk management of the legislative changes.
- ☐ Develop a new IT strategic plan that encompasses the new legislation.

Licensed to Berend Post berend.post@it-university.nl

Question 532

The BEST data backup strategy for mobile users is to:

- ☒ synchronize data directories automatically over the network.
- ☐ have them regularly back up data directories onto CD and courier the backups to the head office.
- ☐ mirror all data to a portable storage device.
- ☐ have them regularly go to branch offices to perform backups.

Question 533

Which of the following should be the MOST important criterion in evaluating a backup solution for sensitive data that must be retained for a long period of time due to regulatory requirements?

- ☐ Full backup window
- ☐ Media costs
- ☐ Restore window
- ☒ Media reliability

Explanation:

Explanation:

To comply with regulatory requirements, the media should be reliable enough to ensure an organization's ability to recovery the data should they be required for any reason. Media price is a consideration, but should not be more important than the ability to provide the required reliability. Choices A and C are less critical than reliability.

Question 534

An IS auditor is involved with a project and finds an IT project stakeholder wants to make a change that could affect both the project scope and schedule. Which of the following would be the MOST appropriate action for the project manager with respect to the change request?

- ☐ Recommend to the project sponsor whether to approve the change
- ☐ Modify the project plan as a result of the change
- ☒ Evaluate the impact of the change
- ☐ Ignore out-of-scope requests

Licensed to Berend Post berend.post@it-university.nl

Question 535

What would be of GREATEST concern to an IS auditor observing shared key cards being utilized to access an organization's data center?

- ☐ The lack of a multi-factor authentication system
- ☒ The inability to identify who has entered the data center
- ☐ The inability to track the number of misplaced cards
- ☐ The lack of enforcement of organizational policy and procedures

Question 536

The use of the Transport Layer Security (TLS) protocol enables the client in a network to be:

- ☐ provided with a digital certificate.
- ☐ identified by a password.
- ☐ registered by the server.
- ☒ assured of the server's identity.

Question 537

Which of the following areas of responsibility would cause the GREATEST segregation of duties conflict if the individual who performs the related tasks also has approval authority?

- ☐ Purchase requisitions and purchase orders
- ☐ Invoices and reconciliations
- ☐ Vendor selection and statements of work
- ☒ Good receipts and payments

Question 538

Which of the following layer of an enterprise data flow architecture is concerned with the assembly and preparation of data for loading into data marts?

- ☒ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Explanation:

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI,

Licensed to Berend Post berend.post@it-university.nl

organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Licensed to Berend Post berend.post@it-university.nl

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

 Licensed to Berend Post berend.post@it-university.nl

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 539

Which of the following would BEST justify spending for a compensating control?

- ☐ Peer benchmarking
- ☒ Risk analysis
- ☐ Threat analysis
- ☐ Vulnerability analysis

Licensed to Berend Post berend.post@it-university.nl

Question 540

An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

- ☒ Staging and job set up
- ☐ Supervisory review of logs
- ☐ Regular back-up of tapes
- ☐ Offsite storage of tapes

Explanation:

Explanation:

If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a compensating control. Choice B is a detective control while choices C and D are corrective controls, none of which would serve as good compensating controls.

Question 541

When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

- ☐ excessive transaction turnaround time.
- ☐ application interface failure.
- ☒ improper transaction authorization.
- ☐ no validated batch totals.

Explanation:

Explanation:

Foremost among the risks associated with electronic data interchange (EDI) is improper transaction authorization. Since the interaction with the parties is electronic, there is no inherent authentication. The other choices, although risks, are not as significant.

Question 542

During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:

- ☐ recommend that the BCP cover all business processes.
- ☒ assess the impact of the processes not covered.
- ☐ report the findings to the IT manager.
- ☐ redefine critical processes.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The business impact analysis needs to be either updated or revisited to assess the risk of not covering all processes in the plan. It is possible that the cost of including all processes might exceed the value of those processes; therefore, they should not be covered. An IS auditor should substantiate this by analyzing the risk.

Question 543

A technology service organization has recently acquired a new subsidiary. What should be the IS auditor's NEXT course of action when considering the impact on the development of the IT audit plan?

- ☐ Review the revised business impact analysis (BIA).
- ☐ Proceed with the current audit plan.
- ☒ Perform a risk assessment.
- ☐ Include the new systems in the audit plan.

Question 544

During an audit of an organization's financial statements, an IS auditor finds that the IT general controls are deficient. What should the IS auditor recommend?

- ☐ Increase the compliance testing of the application controls.
- ☐ Place greater reliance on the application controls.
- ☒ Increase the substantive testing of the financial balances.
- ☐ Place greater reliance on the framework of control.

Question 545

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

- ☐ Results from a business impact analysis
- ☒ Results from a gap analysis
- ☐ An inventory of security controls currently in place
- ☐ Deadline and penalties for noncompliance

Licensed to Berend Post berend.post@it-university.nl

Question 546

Which of the following should be PRIMARILY included in a security training program for business process owners?

- ☐ Application vulnerabilities
- ☐ List of security incidents reported
- ☐ Application recovery time
- ☒ Impact of security risks

Question 547

Which of the following should be an IS auditor's PRIMARY focus when developing a risk-based IS audit program?

- ☐ Business plans
- ☐ Business processes
- ☒ IT strategic plans
- ☐ Portfolio management

Question 548

Which of the following would be the MOST likely reason for an intrusion prevention system (IPS) being unable to block an ongoing web attack?

- ☐ The firewall is not configured properly.
- ☐ The network design contains flaws.
- ☐ Monitoring personnel are not proactive.
- ☒ Signatures are outdated.

Question 549

The sender of a public key would be authenticated by a:

- ☐ certificate authority,
- ☐ digital signature.
- ☒ digital certificate.
- ☐ registration authority.

Explanation:

Explanation:

A digital certificate is an electronic document that declares a public key holder is who the holder claims to be. The certificates do handle data authentication as they are used to determine who sent a particular message. A certificate authority issues the digital certificates, and distributes, generates and manages public keys. A digital signature is used to ensure integrity of the message being sent and solve the nonrepudiation issue of message origination. The registration authority would perform most of the administrative tasks of a certificate authority, i.e., registration of the users of a digital signature plus authenticating the information that is put in the digital certificate.

Licensed to Berend Post berend.post@it-university.nl

Question 550

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a pattern of behaviors, effects, assumptions, attitude and ways of doing things?

- ☐ Governing
- ☒ Culture
- ☐ Enabling and support
- ☐ Emergence

Explanation:

Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

For your exam you should know the information below.

Business Model for Information Security

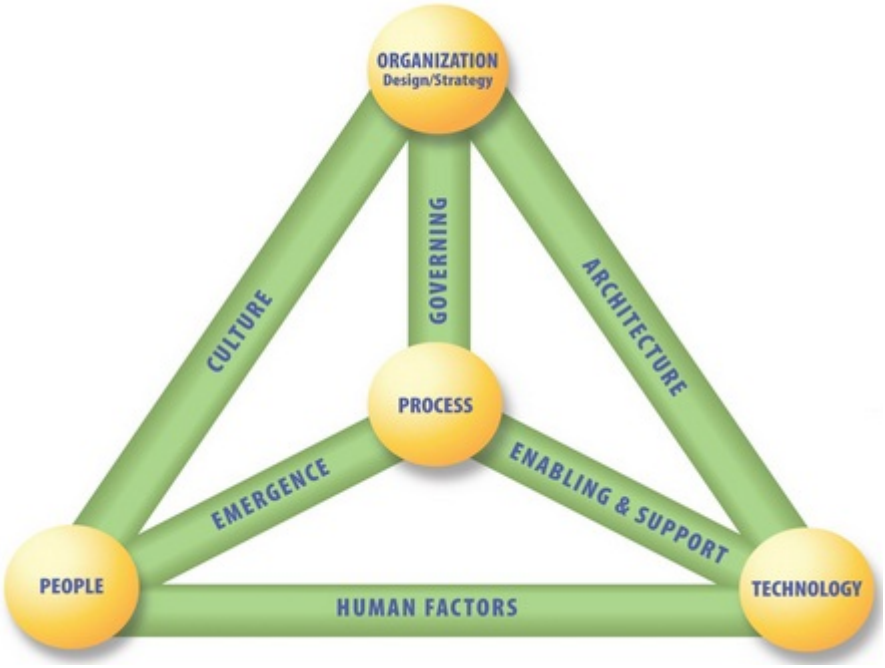
The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. “Systems thinking” is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why “the whole is more than the sum of its parts.” Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist

Licensed to Berend Post berend.post@it-university.nl

the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.

All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

Licensed to Berend Post berend.post@it-university.nl

1. Organization Design and Strategy—An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People—The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:

Recruitment strategies (access, background checks, interviews, roles and responsibilities)

Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)

Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process—Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.

Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology—Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.

Licensed to Berend Post berend.post@it-university.nl

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing—Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

2. Culture—Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support—The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence—Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops;

Licensed to Berend Post berend.post@it-university.nl

alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5. Human factors—The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.

6. Architecture—A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Emergence - Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops;

Licensed to Berend Post berend.post@it-university.nl

alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 37 and 38

http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

Question 551

From a risk management perspective, which of the following is MOST important to be tracked in continuous monitoring?

- ☐ Number of prevented attacks
- ☒ Changes in the threat environment
- ☐ Changes in user privileges
- ☐ Number of failed logins

Question 552

An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

- ☒ Network workstations are not disabled automatically after a period of inactivity.
- ☐ Wiring closets are left unlocked
- ☐ Network operating manuals and documentation are not properly secured.
- ☐ Network components are not equipped with an uninterruptible power supply.

Explanation:

Explanation:

Choice A is the only logical security finding. Network logical security controls should be in place to restrict, identify, and report authorized and unauthorized users of the network. Disabling inactive workstations restricts users of the network. Choice D is an environmental issue and choices B and C are physical security issues. Choices B, C and D should be reported to the appropriate entity.

Licensed to Berend Post berend.post@it-university.nl

Question 553

Which of the following refers to a method of bypassing normal system authentication procedures?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☒ backdoor
- ☐ None of the choices.

Explanation:

Explanation:

A backdoor is a method of bypassing normal authentication procedures.

Many computer manufacturers used to preinstall backdoors on their systems to provide technical support for customers. Hackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors, hackers prefer to use either Trojan horse or computer worm.

Question 554

A multinational organization is integrating its existing payroll system with a human resource information system. Which of the following should be of GREATEST concern to the IS auditor?

- ☐ System documentation
- ☒ Currency conversion
- ☐ Application interfaces
- ☐ Scope creep

Question 555

Which of the following is the MOST important issue for an IS auditor to consider with regard to VoIP communications?

- ☐ Continuity of service
- ☐ Homogeneity of the network
- ☐ Nonrepudiation
- ☒ Identity management

Licensed to Berend Post berend.post@it-university.nl

Question 556

In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

- ☒ Approve and document the change the next business day
- ☐ Limit developer access to production to a specific timeframe
- ☐ Obtain secondary approval before releasing to production
- ☐ Disable the compiler option in the production machine

Explanation:

Explanation:

It may be appropriate to allow programmers to make emergency changes as long as they are documented and approved after the fact. Restricting release time frame may help somewhat; however, it would not apply to emergency changes and cannot prevent unauthorized release of the programs. Choices C and D are not relevant in an emergency situation.

Question 557

Which of the following statement correctly describes the difference between total flooding and local application extinguishing agent?

- ☐ The local application design contain physical barrier enclosing the fire space where as physical barrier is not present in total flooding extinguisher
- ☒ The total flooding design contain physical barrier enclosing the fire space where as physical barrier is not present in local application design extinguisher
- ☐ The physical barrier enclosing fire space is not present in total flooding and local application extinguisher agent
- ☐ The physical barrier enclosing fire space is present in total flooding and local application extinguisher agent

Explanation:

For CISA exam you should know below information about Fire Suppression Systems

Fire Suppression System

This system is designed to automatically activate immediately after detection of heat, typically generated by fire. Like smoke detectors, the system will produce an audible alarm when activated and be linked to a central guard station that is regularly monitored. The system should also be inspected and tested annually. Testing interval should comply with industry and insurance standard and guideline.

Broadly speaking there are two methods for applying an extinguisher agent: total flooding and local application.

Licensed to Berend Post berend.post@it-university.nl

Total Flooding - System working under total flooding application apply an extinguishing agent to a three dimensional enclosed space in order to achieve a concentration of the agent (volume percentage of agent in air) adequate to extinguish the fire. These type of system may be operated automatically by detection and related controls or manually by the operation of a system actuator.

Local Application - System working under a local application principle apply an extinguishing agent directly onto a fire (usually a two dimensional area) or into a three dimensional region immediately surrounding the substance or object on a fire. The main difference between local application and total flooding design is the absence of physical barrier enclosing the fire space in the local application design.

The medium of fire suppression varies but usually one of the following:

Water based systems are typically referred to as sprinkler system. These systems are effective but are also unpopular because they damage equipment and property. The system can be dry-pipe or charged (water is always in system piping). A charged system is more reliable but has the disadvantage of exposing the facility to expensive water damage if the pipe leak or break.

Dry-pipe sprinkling system do not have water in the pipe until an electronic fire alarm activates the water to send water into system. This is opposed to fully charged water pipe system. Dry-pipe system has the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above. Since water and electricity do not mix these systems must be combined with an automatic switch to shut down the electric supply to the area protected.

Holon system releases pressurize halos gases that removes oxygen from air, thus starving the fire. Holon was popular because it is an inert gas and does not damage and does not damage equipment like water does. Because halos adversely affect the ozone layer, it was banned in Montreal (Canada) protocol 1987, which stopped Holon production as of 1 January 1994. As a banned gas, all Holon installation are now required by international agreement to be removed. The Holon substitute is FM-200, which is the most effective alternative.

FM-220TM: Also called heptafluoropropane, HFC-227 or HFC-227ea(ISO Name)is a colorless odorless gaseous fire suppression agent. It is commonly used as a gaseous fire suppression agent.

Aragonite is the brand name for a mixture of 50% argon and 50% nitrogen. It is an inert gas used in gaseous fire suppression systems for extinguishing fires where damage to equipment is to be avoided. Although argon is a nontoxic, it does not satisfy the body's need for oxygen and is simple asphyxiate.

Licensed to Berend Post berend.post@it-university.nl

CO2 system releases pressurized carbon dioxide gas into the area protected to replace the oxygen required for combustion. Unlike halos and its later replacement, however, CO2 is unable to sustain human life. Therefore, in most of countries it is illegal to for such a system to be set to automatic release if any human may be in the area. Because of this, these systems are usually discharged manually, introducing an additional delay in combating fire.

The following were incorrect answers:

The other presented options do not describe valid difference between total flooding and local application extinguishing agent.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 373 and 374

Question 558

Who assumes ownership of a systems-development project and the resulting system?

- ☒ User management
- ☐ Project steering committee
- ☐ IT management
- ☐ Systems developers

Explanation:

Explanation:

User management assumes ownership of a systems-development project and the resulting system.

Question 559

During a follow-up audit, an IS auditor concludes that a previously identified issue has not been adequately remediated. The auditee insists the risk has been addressed. The auditor should:

- ☒ recommend an independent assessment by a third party
- ☐ report the disagreement according to established procedures
- ☐ follow-up on the finding next year
- ☐ accept the auditee's position and close the finding

Licensed to Berend Post berend.post@it-university.nl

Question 560

During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

- ☐ Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
- ☐ Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle.
- ☐ No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
- ☒ Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management.

Explanation:

Explanation:

Establishing regular meetings is the best way to identify and assess risks in a medium- sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organization would normally not have a separate IT risk management department. Moreover, the risks are usually manageable enough so that external help would not be needed. While common risks may be covered by common industry standards, they cannot address the specific situation of an organization. Individual risks will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

Question 561

Which of the following should be performed immediately after a computer security incident has been detected and analyzed by an incident response team?

- ☐ Assess the impact of the incident on critical systems
- ☒ Categorize the incident
- ☐ Eradicate the component that caused the incident
- ☐ Contain the incident before it spreads

Question 562

An IS auditor has been asked to advise on the design and implementation of IT management best practices. Which of the following actions would impair the auditor’s independence?

- ☒ Providing consulting advice for managing applications
- ☐ Designing an embedded audit module
- ☐ Implementing risk response on management’s behalf
- ☐ Evaluating the risk management process

Licensed to Berend Post berend.post@it-university.nl

Question 563

The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

- ☐ achieve performance improvement.
- ☐ provide user authentication.
- ☒ ensure availability of data.
- ☐ ensure the confidentiality of data.

Explanation:

Explanation:

RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication and does nothing to provide for data confidentiality.

Question 564

Which of the following is the INCORRECT "layer - protocol data unit (PDU)" mapping within the TCP/IP model?

- ☐ Application layer – Data
- ☐ Transport layer – Segment
- ☒ Network layer – Frame
- ☐ Physical layer – bits

Explanation:

The word INCORRECT is the keyword used in the question. You need to find out incorrect layer-protocol mapping from give options.

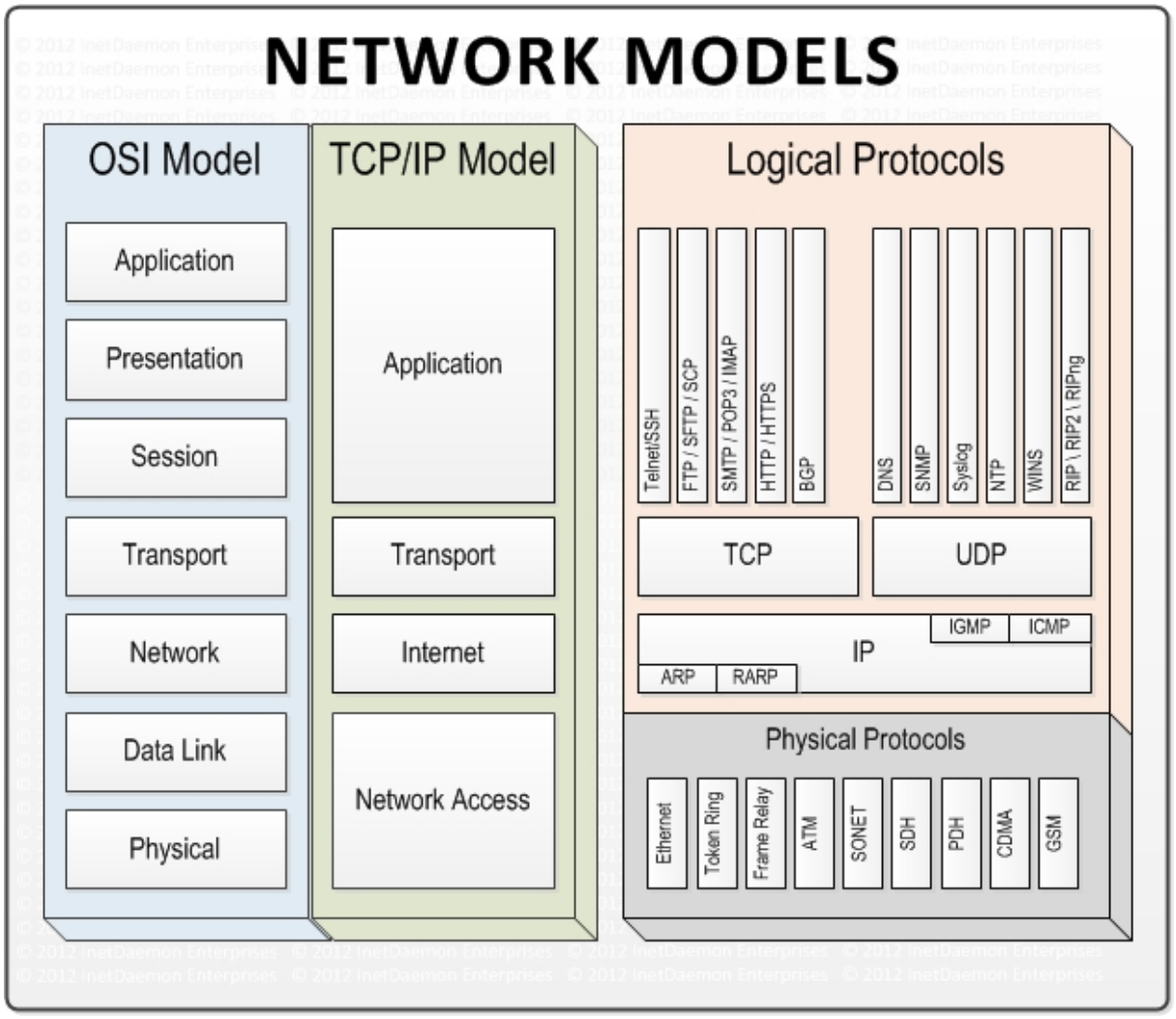
The correct mapping is Network layer – Packet.

The LAN or WAN interface layer creates frame.

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

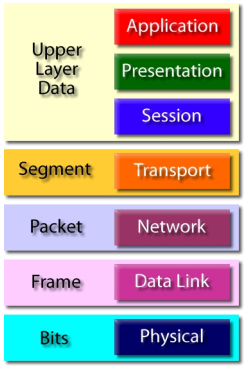
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe layer-PDU mapping in TCP/IP protocol.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 565

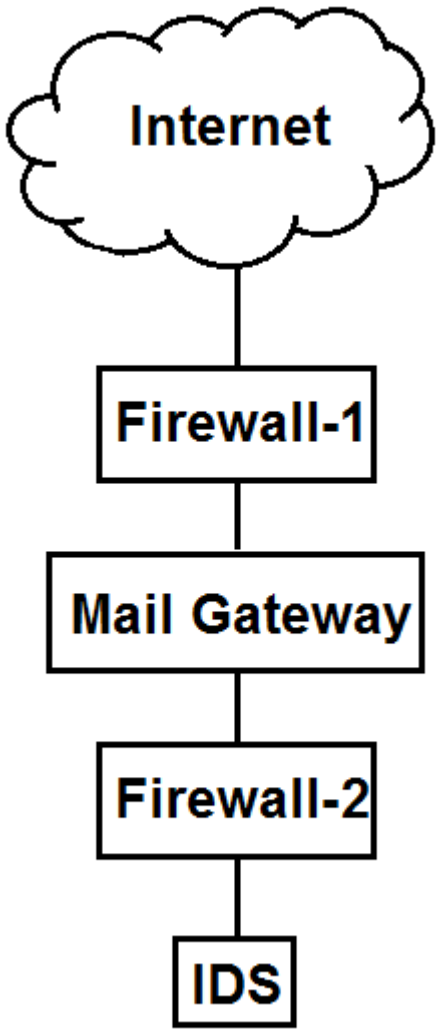
An IS auditor has found that a vendor has gone out of business and the escrow has an older version of the source code. What is the auditor's BEST recommendation for the organization?

- ☐ Continue using the existing application since it meets the current requirements
- ☐ Prepare a maintenance plan that will support the application using the existing code
- ☐ Bring the escrow version up to date
- ☒ Undertake an analysis to determine the business risk

Licensed to Berend Post berend.post@it-university.nl

Question 566

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- ☐ alert the appropriate staff.
- ☐ create an entry in the log.
- ☒ close firewall-2.
- ☐ close firewall-1.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been caused by an attack from a hacker. Closing firewall-2 is the first thing that should be done, thus preventing damage to the internal network.

After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

Question 567

When testing segregation of duties, which of the following audit techniques provides the MOST reliable evidence?

- ☒ Observing daily operations for the area in scope
- ☐ Evaluating the department structure via the organizational chart
- ☐ Reviewing departmental procedure handbooks
- ☐ Interviewing managers and end users

Question 568

The PRIMARY reason for allocating sufficient time between the "go-live" phase of a new system and conducting a post-implementation review is to:

- ☐ update project requirements and design documentation
- ☐ increase availability of system implementation team resources
- ☒ allow the system to stabilize in production
- ☐ obtain sign-off on the scope of post-implementation review

Question 569

When implementing an IT governance framework in an organization the MOST important objective is:

- ☒ IT alignment with the business.
- ☐ accountability.
- ☐ value realization with IT.
- ☐ enhancing the return on IT investments.

Explanation:

Explanation:

The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business {choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

Licensed to Berend Post berend.post@it-university.nl

Question 570

The PRIMARY purpose of audit trails is to:

- ☐ improve response time for users.
- ☒ establish accountability and responsibility for processed transactions.
- ☐ improve the operational efficiency of the system.
- ☐ provide useful information to auditors who may wish to track transactions

Explanation:

Explanation:

Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space.

Question 571

Which of the following is the BEST approach to identify noncompliance issues with legal, regulatory, and contractual requirements?

- ☐ Vulnerability assessment
- ☐ Risk assessment
- ☐ Business impact analysis (BIA)
- ☒ Gap analysis

Question 572

What is an IS auditor's BEST course of action when provided with a status update indicating audit recommendations related to segregation of duties for financial staff have been implemented?

- ☒ Verify sufficient segregation of duties controls are in place.
- ☐ Request documentation of the segregation of duties policy and procedures.
- ☐ Note the department's response in the audit workpapers and records.
- ☐ Confirm with the business that the recommendations are implemented.

Licensed to Berend Post berend.post@it-university.nl

Question 573

A shared resource matrix is a technique commonly used to locate:

- ☐ Malicious code
- ☐ Security flaws
- ☐ Trap doors
- ☒ Covert channels

Explanation:

Explanation:

Analyzing resources of a system is one standard for locating covert channels because the basis of a covert channel is a shared resource.

The following properties must hold for a storage channel to exist:

1. Both sending and receiving process must have access to the same attribute of a shared object.

2. The sending process must be able to modify the attribute of the shared object.

3. The receiving process must be able to reference that attribute of the shared object.

4. A mechanism for initiating both processes and properly sequencing their respective accesses to the shared resource must exist.

Note: Similar properties for timing channel can be listed

The following answers are incorrect:

All other answers were not directly related to discovery of Covert Channels.

The following reference(s) were/was used to create this question:

Acerbic Publications, Acerbic Publications (Test Series) - CRC Press LLC, Page No. 225

http://www.cs.ucsb.edu/~sherwood/cs290/papers/covert-kemmerer.pdf

http://www.cs.utexas.edu/~byoung/cs361/lecture16.pdf

http://www.cs.utexas.edu/~byoung/cs361/lecture16.pdf

Licensed to Berend Post berend.post@it-university.nl

Question 574

A business has requested an IS audit to determine whether information stored in an application system is adequately protected. Which of the following is the MOST important action before the audit work begins?

- ☒ Establish control objectives
- ☐ Conduct a vulnerability analysis
- ☐ Perform penetration testing
- ☐ Review remediation reports

Question 575

Which of the following is the BEST approach for determining the maturity level of an information security program?

- ☐ Review internal audit results.
- ☐ Engage a third-party review.
- ☐ Perform a self-assessment.
- ☒ Evaluate key performance indicators (KPIs).

Question 576

Which of the following BEST describes a common risk in implementing a new application software package?

- ☐ Parameter settings are incorrect
- ☐ Transaction volume is excessive
- ☐ Sensitivity of transactions is high
- ☒ The application lacks audit trails

Question 577

Disaster recovery planning for network connectivity to a hot site over a public-switched network would be MOST likely to include:

- ☐ minimizing the number of points of presence
- ☐ contracts for acquiring new leased lines
- ☐ reciprocal agreements with customers of that network
- ☒ redirecting private virtual circuits

Licensed to Berend Post berend.post@it-university.nl

Question 578

An IS auditor needs to consider many factors while evaluating an encryption system. Which of the following is LEAST important factor to be considered while evaluating an encryption system?

- ☐ Encryption algorithm
- ☐ Encryption keys
- ☐ Key length
- ☒ Implementation language

Explanation:

Implementation language is LEAST important as compare to other options. Encryption algorithm, encryption keys and key length are key elements of an Encryption system.

It is important to read carefully the question. The word "LEAST" was the key word. You had to find which one was LEAST important.

The following were incorrect answers:

Other options mentioned are key elements of an Encryption system

Encryption Algorithm – A mathematically based function or calculation that encrypts/decrypts data

Encryption keys – A piece of information that is used within an encryption algorithm (calculation) to make encryption or decryption process unique. Similar to passwords, a user needs to use the correct key to access or decipher the message into an unreadable form.

Key length – A predetermined length for the key. The longer the key, the more difficult it is to compromise in brute-force attack where all possible key combinations are tried.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

Licensed to Berend Post berend.post@it-university.nl

Question 579

Which of the following is the client organization's responsibility in a Software as a Service (SaaS) environment?

- ☐ Detecting unauthorized access
- ☒ Ensuring that users are properly authorized
- ☐ Ensuring the data is available when needed
- ☐ Preventing insertion of malicious code

Question 580

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following MUST be in place for this solution to be relevant to the organization?

- ☐ An adequate data testing environment
- ☐ Senior management support
- ☒ A business case
- ☐ A data classification

Question 581

What is the BEST approach to mitigate the risk of a phishing attack?

- ☐ implement an intrusion detection system (IDS)
- ☐ Assess web site security
- ☐ Strong authentication
- ☒ User education

Explanation:

Explanation:

Phishing attacks can be mounted in various ways; intrusion detection systems (IDSs) and strong authentication cannot mitigate most types of phishing attacks. Assessing web site security does not mitigate the risk. Phishing uses a server masquerading as a legitimate server. The best way to mitigate the risk of phishing is to educate users to take caution with suspicious internet communications and not to trust them until verified. Users require adequate training to recognize suspicious web pages and e-mail.

Question 582

Which of the following MOST effectively prevents internal users from modifying sensitive data?

- ☐ Network segmentation
- ☐ Multi-factor authentication
- ☐ Acceptable use policies
- ☒ Role-based access controls

Licensed to Berend Post berend.post@it-university.nl

Question 583

When reviewing a hardware maintenance program, an IS auditor should assess whether:

- ☐ the schedule of all unplanned maintenance is maintained.
- ☐ it is in line with historical trends.
- ☐ it has been approved by the IS steering committee.
- ☒ the program is validated against vendor specifications.

Explanation:

Explanation: Though maintenance requirements vary based on complexity and performance workloads, a hardware maintenance schedule should be validated against the vendor-provided specifications. For business reasons, an organization may choose a more aggressive maintenance program than the vendor's program. The maintenance program should include maintenance performance history, be it planned, unplanned, executed or exceptional. Unplanned maintenance cannot be scheduled. Hardware maintenance programs do not necessarily need to be in line with historical trends. Maintenance schedules normally are not approved by the steering committee.

Question 584

An organization has suffered a number of incidents in which USB flash drives with sensitive data have been lost. Which of the following would be MOST effective in preventing loss of sensitive data?

- ☐ Modifying the disciplinary policy to be more stringent
- ☐ Implementing a check-in/check-out process for USB flash drives
- ☒ Issuing encrypted USB flash drives to staff
- ☐ Increasing the frequency of security awareness training

Question 585

An internal IS auditor recommends that incoming accounts payable payment files be encrypted. Which type of control is the auditor recommending?

- ☐ Corrective
- ☐ Detective
- ☐ Preventive
- ☒ Directive

Question 586

An IS auditor finds that a company is using a payroll provider hosted in a foreign country. Of the following, the MOST important audit consideration is whether the provider’s operations:

- ☐ meet industry best practice and standards
- ☒ comply with applicable laws and regulations
- ☐ are shared with other companies using the provider
- ☐ are aligned with the company’s culture

Licensed to Berend Post berend.post@it-university.nl

Question 587

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

- ☐ testing stage.
- ☐ evaluation stage.
- ☐ maintenance stage.
- ☒ early stages of planning.

Explanation:

Explanation:

Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

Question 588

John had implemented a validation check on the marital status field of a payroll record. A payroll record contains a field for marital status and acceptable status code are M for Married or S for Single. If any other code is entered, record should be rejected. Which of the following data validation control was implemented by John?

- ☐ Range Check
- ☒ Validity Check
- ☐ Existence check
- ☐ Reasonableness check

Explanation:

In a validity check control programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Licensed to Berend Post berend.post@it-university.nl

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Licensed to Berend Post berend.post@it-university.nl

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 215

Question 589

An IS auditor plans to review all access attempts to a video-monitored and proximity card-controlled communications room. Which of the following would be MOST useful to the auditor?

- ☒ System electronic log
- ☐ Security incident log
- ☐ Manual sign-in and sign-out log
- ☐ Alarm system with CCTV

Explanation:

Reference: https://www.slideshare.net/desmond.devendran/chap5-2007-cisa-review-course

Licensed to Berend Post berend.post@it-university.nl

Question 590

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

- ☐ The recipient uses their private key to decrypt the secret key.
- ☐ The encrypted prehash code and the message are encrypted using a secret key.
- ☐ The encrypted prehash code is derived mathematically from the message to be sent.
- ☒ The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.

Explanation:

Explanation:

Most encrypted transactions use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or recipient. The recipient uses the sender's public key to decrypt the prehash code into a posthash code, which when equaling the prehash code, verifies the identity of the sender and that the message has not been changed in route; this would provide the greatest assurance. Each sender and recipient has a private key known only to themselves and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key, and both must be from the same party. A single, secret key is used to encrypt the message, because secret key encryption requires less processing power than using public and private keys. A digital certificate, signed by a certificate authority, validates senders' and recipients' public keys.

Question 591

An organization's IT department is undertaking a large virtualization project to reduce its physical server footprint. Which of the following should be the HIGHEST priority of the information security manager?

- ☐ Determining how incidents will be managed
- ☐ Selecting the virtualization software
- ☒ Being involved as the design stage of the project
- ☐ Ensuring the project has appropriate security funding

Question 592

Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

- ☐ Proxy server
- ☐ Firewall installation
- ☐ Network administrator
- ☒ Password implementation and administration

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The most comprehensive control in this situation is password implementation and administration. While firewall installations are the primary line of defense, they cannot protect all access and,

therefore, an element of risk remains. A proxy server is a type of firewall installation; thus, the same rules apply. The network administrator may serve as a control, but typically this would not be comprehensive enough to serve on multiple and diverse systems.

Question 593

Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?

- ☐ Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
- ☐ During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
- ☐ The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
- ☒ Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Explanation:

Explanation:

A disaster recovery test should test the plan, processes, people and IT systems. Therefore, if the plan is not used, its accuracy and adequacy cannot be verified. Disaster recovery should not rely on key staff since a disaster can occur when they are not available. It is common that not all systems can be tested in a limited test time frame. It is important, however, that those systems which are essential to the business are tested, and that the other systems are eventually tested throughout the year. One aim of the test is to identify and replace defective devices so that all systems can be replaced in the case of a disaster. Choice B would only be a concern if the number of discovered problems is systematically very high, in a real disaster, there is no need for a clean shutdown of the original production environment since the first priority is to bring the backup site up.

Question 594

Most access violations are:

- ☒ Accidental
- ☐ Caused by internal hackers
- ☐ Caused by external hackers
- ☐ Related to Internet

Explanation:

The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

Licensed to Berend Post berend.post@it-university.nl

Question 595

An IS auditor is evaluating the log management system for an organization with devices and systems in multiple geographic locations. Which of the following is MOST important for the auditor to verify?

- ☐ Log files are encrypted and digitally signed.
- ☒ Log files of the servers are synchronized.
- ☐ Log files are reviewed in multiple locations.
- ☐ Log files are concurrently updated.

Question 596

During an annual security review of an organization's servers, it was found that the customer service team's file server, which contains sensitive customer data, is accessible to all user IDs in the organization. Which of the following should the information security manager do FIRST?

- ☒ Report the situation to the data owner.
- ☐ Remove access privileges to the folder containing the data.
- ☐ Train the customer service team on properly controlling file permissions.
- ☐ Isolate the server from the network.

Question 597

A company is planning to implement a new administrative system at many sites. The new system contains four integrated modules. Which of the following implementation approaches would be MOST appropriate?

- ☐ Parallel implementation module by module
- ☒ Pilot run of the new system
- ☐ Full implementation of the new system
- ☐ Parallel run at all locations

Question 598

The FIRST step in managing the risk of a cyber-attack is to:

- ☐ assess the vulnerability impact.
- ☐ evaluate the likelihood of threats.
- ☒ identify critical information assets.
- ☐ estimate potential damage.

Explanation:

Explanation:

The first step in the managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

Licensed to Berend Post berend.post@it-university.nl

Question 599

Which of the following is the GREATEST risk of cloud computing?

- ☐ Reduced performance
- ☒ Disclosure of data
- ☐ Lack of scalability
- ☐ Inflexibility

Question 600

Which of the following should the IS auditor use to BEST determine whether a project has met its business objectives?

- ☐ Earned-value analysis
- ☐ Completed project plan
- ☐ Issues log with resolutions
- ☒ Benefits realization document

Question 601

In an organization that has undergone an expansion through an acquisition, which of the following would BEST secure the enterprise network?

- ☐ Business or role-based segmentation
- ☒ Using security groups
- ☐ Log analysis of system access
- ☐ Encryption of data traversing networks.

Question 602

An IS auditor can BEST help management fulfill risk management responsibilities by:

- ☐ highlighting specific risks not being addressed.
- ☐ ensuring the roles for managing IT risk are defined.
- ☒ developing an IT risk management framework.
- ☐ adopting a mechanism for reporting issues.

Licensed to Berend Post berend.post@it-university.nl

Question 603

An organization has an approved bring your own device (BYOD) program. Which of the following is the MOST effective method to enforce application control on personal devices?

- ☒ Implement a mobile device management solution.
- ☐ Establish a mobile device acceptable use policy.
- ☐ Implement a web application firewall.
- ☐ Educate users regarding the use of approved applications.

Question 604

A retailer normally uses a scanner to read product labels and input product codes and prices. The unit is not functioning and staff are keying information manually. With respect to the accuracy of the input, it is likely that:

- ☒ audit risk has increased.
- ☐ control risk has increased.
- ☐ inherent risk has decreased.
- ☐ detection risk has decreased.

Question 605

Which of the following term related to network performance refers to the delay that packet may experience on their way to reach the destination from the source?

- ☐ Bandwidth
- ☐ Throughput
- ☒ Latency
- ☐ Jitter

Explanation:

Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

The latency assumption seems to be that data should be transmitted instantly between one point and another (that is, with no delay at all). The contributors to network latency include:

Propagation: This is simply the time it takes for a packet to travel between one place and another at the speed of light.

Licensed to Berend Post berend.post@it-university.nl

Transmission: The medium itself (whether optical fiber, wireless, or some other) introduces some delay. The size of the packet introduces delay in a round trip since a larger packet will take longer to receive and return than a short one.

Router and other processing: Each gateway node takes time to examine and possibly change the header in a packet (for example, changing the hop count in the time-to-live field).

Other computer and storage delays: Within networks at each end of the journey, a packet may be subject to storage and hard disk access delays at intermediate devices such as switches and bridges. (In backbone statistics, however, this kind of latency is probably not considered.)

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

 Licensed to Berend Post berend.post@it-university.nl

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 275

Question 606

An organization considers implementing a system that uses a technology that is not in line with the organization's IT strategy. Which of the following is the BEST justification for deviating from the IT strategy?

- ☒ The system has a reduced cost of ownership.
- ☐ The organization has staff familiar with the technology.
- ☐ The business benefits are achieved even with extra costs.
- ☐ The system makes use of state-of-the-art technology.

Question 607

An IS auditor finds that periodic reviews of read-only users for a reporting system are not being performed. Which of the following should be the IS auditor's NEXT course of action?

- ☐ Obtain a verbal confirmation from IT for this exemption.
- ☐ Review the list of end-users and evaluate for authorization.
- ☒ Verify management's approval for this exemption.
- ☐ Report this control process weakness to senior management.

Licensed to Berend Post berend.post@it-university.nl

Question 608

Which of the following represents the GREATEST potential risk in an EDI environment?

- ☒ Transaction authorization
- ☐ Loss or duplication of EDI transmissions
- ☐ Transmission delay
- ☐ Deletion or manipulation of transactions prior to or after establishment of application controls

Explanation:

Explanation:

Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

Question 609

Which of the following findings would be of GREATEST concern to an IS auditor reviewing an organization's newly implemented online security awareness program?

- ☐ Only new employees are required to attend the program
- ☐ The timing for program updates has not been determined
- ☒ Metrics have not been established to assess training results
- ☐ Employees do not receive immediate notification of results

Question 610

Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

- ☐ Encrypts the information transmitted over the network
- ☒ Makes other users' certificates available to applications
- ☐ Facilitates the implementation of a password policy
- ☐ Stores certificate revocation lists (CRLs)

Explanation:

Explanation:

A directory server makes other users' certificates available to applications. Encrypting the information transmitted over the network and storing certificate revocation lists (CRLs) are roles performed by a security server. Facilitating the implementation of a password policy is not relevant to public key infrastructure (PKI).

Licensed to Berend Post berend.post@it-university.nl

Question 611

In a public key infrastructure, a registration authority:

- ☒ verifies information supplied by the subject requesting a certificate.
- ☐ issues the certificate after the required attributes are verified and the keys are generated.
- ☐ digitally signs a message to achieve nonrepudiation of the signed message.
- ☐ registers signed messages to protect them from future repudiation.

Explanation:

Explanation:

A registration authority is responsible for verifying information supplied by the subject requesting a certificate, and verifies the requestor's right to request certificate attributes and that the requestor actually possesses the private key corresponding to the public key being sent.

Certification authorities, not registration authorities, actually issue certificates once verification of the information has been completed; because of this, choice B is incorrect. On the other hand, the sender who has control of their private key signs the message, not the registration authority. Registering signed messages is not a task performed by registration authorities.

Question 612

An organization's data retention policy states that all data will be backed up, retained for 10 years, and then destroyed. When conducting an audit of the long-term offsite backup program, an IS auditor should:

- ☐ verify that business owners review data before it is destroyed.
- ☒ verify that there is a process to ensure readability and restore capability.
- ☐ confirm that business interruption insurance coverage is in place.
- ☐ review data classification schemes for appropriate security levels.

Question 613

When auditing the effectiveness of a biometric system, which of the following indicators would be MOST important to review?

- ☐ False negatives
- ☒ False acceptance rate
- ☐ Failure to enroll rate
- ☐ System response time

Licensed to Berend Post berend.post@it-university.nl

Question 614

Which of the following is the MOST important requirement for an IS auditor to evaluate when reviewing a transmission of personally identifiable information (PII) between two organizations?

- ☐ Completeness
- ☐ Timeliness
- ☒ Necessity
- ☐ Accuracy

Question 615

One advantage of monetary unit sampling is the fact that:

- ☒ results are stated in terms of the frequency of items in error
- ☐ it can easily be applied manually when computer resources are not available
- ☐ it increases the likelihood of selecting material items from the population
- ☐ large-value population items are segregated and audited separately

Question 616

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- ☒ address audit objectives.
- ☐ collect sufficient evidence.
- ☐ specify appropriate tests.
- ☐ minimize audit resources.

Explanation:

Explanation:

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

Question 617

Which of the following should be the PRIMARY concern of an IS auditor during a review of an external IT service level agreement (SLA) for computer operations?

- ☐ No employee succession plan
- ☒ Changes in services are not tracked
- ☐ Lack of software escrow provisions
- ☐ Vendor has exclusive control of IT resources

Licensed to Berend Post berend.post@it-university.nl

Question 618

An IS auditor reviewing the acquisition of new equipment would consider which of the following to be a significant weakness?

- ☐ Staff involved in the evaluation were aware of the vendors being evaluated.
- ☐ Independent consultants prepared the request for proposal (RFP) documents.
- ☒ Evaluation criteria were finalized after the initial assessment of responses.
- ☐ The closing date for responses was extended after a request from potential vendors.

Question 619

Which of the following is the MOST important control to implement when senior managers use smartphones to access sensitive company information?

- ☐ Mandatory virtual private network (VPN) connectivity
- ☐ Centralized device administration
- ☐ Strong passwords
- ☒ Anti-malware on the devices

Question 620

Change control for business application systems being developed using prototyping could be complicated by the:

- ☐ iterative nature of prototyping.
- ☒ rapid pace of modifications in requirements and design.
- ☐ emphasis on reports and screens.
- ☐ lack of integrated tools.

Explanation:

Explanation:

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

Question 621

What should the information security manager do FISRT when end users express that new security controls are too restrictive?

- ☒ Perform a risk assessment on modifying the control environment.
- ☐ Perform a cost-benefit analysis on modifying the control environment.
- ☐ Conduct a business impact analysis (BIA).
- ☐ Obtain process owner buy-in to remove the controls.

Licensed to Berend Post berend.post@it-university.nl

Question 622

Which of the following statement correctly describes difference between SSL and S/HTTP?

- ☐ Both works at application layer of OSI model
- ☒ SSL works at transport layer where as S/HTTP works at application layer of OSI model
- ☐ Both works at transport layer
- ☐ S/HTTP works at transport layer where as SSL works at the application layer of OSI model

Explanation:

For your exam you should know below information about S/HTTP and SSL protocol:

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) - These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases

Peer negotiation for algorithm support

Public-key, encryption based key exchange and certificate based authentication

Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

Licensed to Berend Post berend.post@it-university.nl

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

The other choices presented in the options are not valid asSSL works at transport layer where as S/HTTP works at application layer of OSI model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352

Question 623

To select a sample for testing, which must include the 80 largest client balances and a random sample of the rest, the IS auditor should recommend:

- ☐ sorting the file with a utility.
- ☐ use of generalized audit software.
- ☒ applying attribute sampling using software.
- ☐ development of an integrated test facility (ITF).

Question 624

A business unit cannot achieve desired segregation of duties between operations and programming due to size constraints. Which of the following is MOST important for the IS auditor to identify?

- ☐ Unauthorized user controls
- ☒ Compensating controls
- ☐ Controls over operational effectiveness
- ☐ Additional control weaknesses

Licensed to Berend Post berend.post@it-university.nl

Question 625

To integrate security into system development life cycle (SDLC) processes, an organization MUST ensure that security:

- ☒ is a prerequisite for completion of major phases.
- ☐ performance metrics have been met.
- ☐ roles and responsibilities have been defined.
- ☐ is represented on the configuration control board.

Question 626

Which of the following is the PRIMARY role of a data custodian?

- ☐ Processing information
- ☒ Securing information
- ☐ Classifying information
- ☐ Validating information

Question 627

An information security manager is preparing an incident response plan. Which of the following is the MOST important consideration when responding to an incident involving sensitive customer data?

- ☐ The assignment of a forensics teams
- ☐ The ability to recover from the incident in a timely manner
- ☒ Following defined post-incident review procedures
- ☐ The ability to obtain incident information in a timely manner

Question 628

Which of the following is the MOST important consideration when deploying closed-circuit television (CCTV) systems that use wireless communication links to transmit images between cameras and a receiver?

- ☐ Encryption of transmissions
- ☒ Monitoring by security guards
- ☐ Retention period of recordings
- ☐ Strategic placement of cameras

Licensed to Berend Post berend.post@it-university.nl

Question 629

After an external IS audit, which of the following should be IT management's MAIN consideration when determining the prioritization of follow-up activities?

- ☐ The amount of time since the initial audit was completed.
- ☒ The materiality of the reported findings
- ☐ The availability of the external auditors
- ☐ The scheduling of major changes in the control environment

Question 630

Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?

- ☐ Identifying risk mitigation options
- ☒ Identifying key business risks
- ☐ Identifying critical business processes
- ☐ Identifying the threat environment

Question 631

Which of the following should be the MOST important consideration when determining which information system application to audit?

- ☐ Cost-benefit analysis
- ☐ Available resources
- ☒ Business impact analysis
- ☐ Newly implemented systems

Question 632

Data confidentiality is a requirement for an organization's new web service. Which of the following would provide the BEST protection?

- ☐ Telnet
- ☐ Secure Sockets Layer (SSL)
- ☒ Transport Layer Security (TLS)
- ☐ Secure File Transfer Protocol (SFTP)

Licensed to Berend Post berend.post@it-university.nl

Question 633

An IS auditor has been asked to audit the proposed acquisition of new computer hardware. The auditor's PRIMARY concern is that:

- ☐ the implementation plan meets user requirements.
- ☐ a clear business case has been established.
- ☒ the new hardware meets established security standards.
- ☐ a full, visible audit trail will be included.

Question 634

Which of the following are the characteristics of a good password?

- ☒ It has mixed-case alphabetic characters, numbers, and symbols.
- ☐ It has mixed-case alphabetic characters and numbers.
- ☐ It has mixed-case alphabetic characters and symbols.
- ☐ It has mixed-case alphabetic characters, numbers, and binary codes.
- ☐ None of the choices.

Explanation:

Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

Question 635

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- ☒ financial results.
- ☐ customer satisfaction.
- ☐ internal process efficiency.
- ☐ innovation capacity.

Explanation:

Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

Licensed to Berend Post berend.post@it-university.nl

Question 636

When developing a risk-based IS audit plan, the PRIMARY focus should be on functions:

- ☐ considered important by IT management.
- ☐ with the most ineffective controls.
- ☐ with the greatest number of threats.
- ☒ considered critical to business operations.

Question 637

When developing a risk-based audit strategy, an IS auditor conduct a risk assessment to ensure that:

- ☐ controls needed to mitigate risks are in place.
- ☒ vulnerabilities and threats are identified.
- ☐ audit risks are considered.
- ☐ a gap analysis is appropriate.

Explanation:

Explanation:

In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage.

Understanding whether appropriate controls required to mitigate risks are in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be done to compare the actual state to an expected or desirable state.

Question 638

An IS auditor is conducting a review of an organization's information systems and discovers data that is no longer needed by business applications. Which of the following would be the IS auditor's BEST recommendation?

- ☒ Ask the data custodian to remove it after confirmation from the business user.
- ☐ Assess the data according to the retention policy.
- ☐ Back up the data to removable media and store in a secure area.
- ☐ Keep the data and protect it using a data classification policy.

Licensed to Berend Post berend.post@it-university.nl

Question 639

An IS auditor is assessing the results of an organization's post-implementation review of a newly developed information system. Which of the following should be the auditor's MAIN focus?

- ☐ The procurement contract has been closed.
- ☐ Lessons learned have been identified.
- ☒ The disaster recovery plan has been updated.
- ☐ Benefits realization analysis has been completed.

Question 640

The BEST way to evaluate the effectiveness of a newly developed application is to:

- ☐ perform a post-implementation review.
- ☐ analyze load-testing results.
- ☒ review acceptance-testing results.
- ☐ perform a pre-implementation review.

Question 641

Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

- ☐ Parallel Test
- ☐ Black box testing
- ☒ Regression Testing
- ☐ Pilot Testing

Explanation:

Regression testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Licensed to Berend Post berend.post@it-university.nl

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

 Licensed to Berend Post berend.post@it-university.nl

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 167

Question 642

Which of the following is the dominating objective of BCP and DRP?

- ☒ To protect human life
- ☐ To mitigate the risk and impact of a business interruption
- ☐ To eliminate the risk and impact of a business interruption
- ☐ To transfer the risk and impact of a business interruption

Explanation:

Explanation:

Although the primary business objective of BCP and DRP is to mitigate the risk and impact of a business interruption, the dominating objective remains the protection of human life.

Question 643

The final acceptance testing of a new application system should be the responsibility of the:

- ☐ IS audit team.
- ☐ user group
- ☐ IS management
- ☒ quality assurance team

Licensed to Berend Post berend.post@it-university.nl

Question 644

Which of the following is the MOST important difference between end-user computing (EUC) applications and traditional applications?

☐ Traditional application documentation is typically less comprehensive than EUC application documentation.
☐ Traditional applications require roll-back procedures whereas EUC applications do not.
☐ Traditional applications require periodic patching whereas EUC applications do not.
☒ Traditional application input controls are typically more robust than EUC application input controls.

Question 645

In which of the following payment mode, the payer creates payment transfer instructions, signs it digitally and sends it to issuer?

☐ Electronic Money Model
☐ Electronics Checks model
☒ Electronic transfer model
☐ Electronic withdraw model

Explanation:

Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems – the issuer and the user. An issuer is an entity that operates the payment service. An issuer holds the items that the payment represents. The user of the payment service performs two main functions- making payments and receiving payments – and therefore can be described as a payer or payee receptively.

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Licensed to Berend Post berend.post@it-university.nl

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

The following were incorrect answers:

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Withdraw Model – Not a valid type of payment system.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 183

Licensed to Berend Post berend.post@it-university.nl

Question 646

What is often the most difficult part of initial efforts in application development?

- ☐ Configuring software
- ☐ Planning security
- ☒ Determining time and resource requirements
- ☐ Configuring hardware

Explanation:

Explanation:

Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

Question 647

Two organizations will share ownership of a new enterprise resource management (ERM) system. To help ensure the successful implementation of the system, it is MOST important to define:

- ☒ access to data
- ☐ the governance model
- ☐ custody of assets
- ☐ appropriate procedures

Question 648

Which of the following is MOST important to the effective management of an end user-developed application?

- ☐ Implementing best practice folder structures
- ☐ Continuous monitoring to facilitate prompt escalation of issues
- ☒ Assigning risk ratings based on probability and impact
- ☐ Stress testing the application through use of data outliers

Question 649

An existing system is being replaced with a new application package. User acceptance testing (UAT) should ensure that:

- ☐ data from the old system has been converted correctly
- ☒ the new system functions as expected
- ☐ the new system is better than the old system
- ☐ there is a business need for the new system

Licensed to Berend Post berend.post@it-university.nl

Question 650

Effective transactional controls are often capable of offering which of the following benefits (Choose four.):

- ☒ reduced administrative and material costs
- ☒ shortened contract cycle times
- ☒ enhanced procurement decisions
- ☒ diminished legal risk
- ☐ None of the choices.

Explanation:

Explanation:

Transactional systems provide a baseline necessary to measure and monitor contract performance and provide a method for appraising efficiency against possible areas of exposure. Effective transactional controls reduce administrative and material costs, shorten contract cycle times, enhance procurement decisions, and diminish legal risk.

Question 651

A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?

- ☒ The system will not process the change until the clerk's manager confirms the change by entering an approval code.
- ☐ The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager.
- ☐ The system requires the clerk to enter an approval code.
- ☐ The system displays a warning message to the clerk.

Explanation:

Explanation:

Choice A would prevent or detect the use of an unauthorized interest rate. Choice B informs the manager after the fact that a change was made, thereby making it possible for transactions to use an unauthorized rate prior to management review. Choices C and D do not prevent the clerk from entering an unauthorized rate change.

Licensed to Berend Post berend.post@it-university.nl

Question 652

In wireless communication, which of the following controls allows the device receiving the communications to verify that the received communications have not been altered in transit?

- ☐ Device authentication and data origin authentication
- ☐ Wireless intrusion detection (IDS) and prevention systems (IPS)
- ☒ The use of cryptographic hashes
- ☐ Packet headers and trailers

Explanation:

Explanation:

Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks. Device authentication and data origin authentication is not the correct answer since authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading. Wireless iDS/IPSs is not the correct answer since wireless IDS/IPS shave the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Packet headers and trailers alone do not ensure that the content has not been altered.

Question 653

Which of the following should be an IS auditor's PRIMARY consideration when evaluating the development and design of a privacy program?

- ☐ Data governance and data classification procedures
- ☐ Policies and procedures consistent with privacy guidelines
- ☒ Industry practice and regulatory compliance guidance
- ☐ Information security and incident management practices

Question 654

Which of the following is the BEST way to protect the confidentiality of data on a corporate smartphone?

- ☐ Disabling public wireless connections
- ☒ Using remote data wipe capabilities
- ☐ Using encryption
- ☐ Changing the default PIN for Bluetooth connections

Licensed to Berend Post berend.post@it-university.nl

Question 655

IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

- ☐ Port scanning
- ☐ Back door
- ☐ Man-in-the-middle
- ☒ War driving

Explanation:

Explanation:

A war driving attack uses a wireless Ethernet card, set in promiscuous mode, and a powerful antenna to penetrate wireless systems from outside. Port scanning will often target the external firewall of the organization. A back door is an opening left in software that enables an unknown entry into a system. Man-in-the-middle attacks intercept a message and either replace or modify it.

Question 656

Which of the following would be the MOST effective method to address software license violations on employee workstations?

- ☒ Restricting administrative rights on employee workstations
- ☐ Requiring automated installation of software
- ☐ Scanning of workstations daily for unauthorized software use
- ☐ Implementing real-time monitoring software on employee workstations

Question 657

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

- ☐ Specific developments only
- ☐ Business requirements only
- ☒ All phases of the installation must be documented
- ☐ No need to develop a customer specific documentation

Explanation:

Explanation:

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

Licensed to Berend Post berend.post@it-university.nl

Question 658

Which of the following should an IS auditor verify when auditing the effectiveness of virus protection?

- ☐ Frequency of IDS log reviews
- ☒ Currency of software patch application
- ☐ Schedule for migration to production
- ☐ Frequency of external Internet access

Question 659

Which of the following correctly describes the purpose of an Electronic data processing audit?

- ☒ to collect and evaluate evidence of an organization's information systems, practices, and operations.
- ☐ to ensure document validity.
- ☐ to verify data accuracy.
- ☐ to collect and evaluate benefits brought by an organization's information systems to its bottom line.
- ☐ None of the choices.

Explanation:

Explanation:

An Electronic data processing (EDP) audit is an IT audit. It is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations.

Question 660

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

- ☐ project be discontinued.
- ☒ business case be updated and possible corrective actions be identified.
- ☐ project be returned to the project sponsor for reapproval.
- ☐ project be completed and the business case be updated later.

Explanation:

Explanation: An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case. The IS auditor should recommend that the business case be kept current throughout the project since it is a key input to decisions made throughout the life of any project.

Licensed to Berend Post berend.post@it-university.nl

Question 661

Which of the following is the GREATEST concern when an organization's disaster recovery strategy utilizes a cold site?

- ☐ The lack of electrical power connections
- ☐ The lack of networking infrastructure
- ☐ The lack of appropriate environmental controls
- ☒ The lack of hardware components availability

Question 662

Before concluding that internal controls can be relied upon, the IS auditor should:

- ☐ discuss the internal control weaknesses with the auditee
- ☐ document application controls
- ☐ conduct tests of compliance
- ☒ document the system of internal control

Question 663

Which of the following characteristics pertaining to databases is not true?

- ☐ A data model should exist and all entities should have a significant name.
- ☒ Justifications must exist for normalized data.
- ☐ No NULLs should be allowed for primary keys.
- ☐ All relations must have a specific cardinality.

Explanation:

Justifications should be provided when data is renormalized, not when it is normalized, because it introduces risk of data inconsistency. Renormalization is usually introduced for performance purposes.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

Question 664

What type of approach to the development of organizational policies is often driven by risk assessment?

- ☐ Bottom-up
- ☒ Top-down
- ☐ Comprehensive
- ☐ Integrated

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A bottom-up approach to the development of organizational policies is often driven by risk assessment.

Question 665

A review of Internet security disclosed that users have individual user accounts with the Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only corporate network is used. The organization should FIRST:

- ☐ use a proxy server to filter out Internet sites that should not be accessed.
- ☐ keep a manual log of Internal access.
- ☐ monitor remote access activities.
- ☒ include a statement in its security policy about Internet use.

Question 666

Which of the following MUST be included in emergency change control procedures?

- ☒ Obtaining user management approval before implementing the changes
- ☐ Updating production source libraries to reflect the changes
- ☐ Using an emergency ID to move production programs into development
- ☐ Requesting that the help desk makes the changes

Question 667

Which of the following is the PRIMARY role of an IS auditor with regard to data privacy?

- ☒ Ensuring compliance with data privacy laws
- ☐ Communicating data privacy requirements to the organization
- ☐ Drafting the organization's data privacy policy
- ☐ Verifying that privacy practices match privacy statements

Question 668

For several years, a vendor has been providing offsite backup media and record storage for a bank. Due to familiarity with bank employees, the vendor does not consistently require authorization forms from them to retrieve media. Which of the following is the GREATEST risk from this situation?

- ☐ Bank employees can inappropriately obtain sensitive records
- ☐ Backup tapes may not be available
- ☒ Chain of custody could not be validated
- ☐ The vendor provides the incorrect media to employees

Licensed to Berend Post berend.post@it-university.nl

Question 669

While reviewing a hot site, the IS auditor discovers that one type of hardware platform is not installed. The IS auditor should FIRST:

- ☐ recommend the purchase and installation of hardware at the hot site.
- ☐ report the finding immediately to senior IS management.
- ☒ determine the business impact of the absence of the hardware.
- ☐ establish the lead time for delivery of a new machine.

Question 670

The PRIMARY purpose of reviewing the IT strategic plan is to identify risks that may:

- ☐ limit the ability to deliver customer requirements.
- ☒ limit the organization's ability to achieve its objectives.
- ☐ impact operational efficiency of the IT department.
- ☐ impact financial resourcing to implement the plan.

Question 671

Talking about application system audit, focus should always be placed on (Choose five.)

- ☒ performance and controls of the system
- ☒ the ability to limit unauthorized access and manipulation
- ☒ input of data are processed correctly
- ☒ output of data are processed correctly
- ☒ changes to the system are properly authorized
- ☐ None of the choices.

Explanation:

Explanation:

Talking about application system audit, focus should be placed on the performance and controls of the system, its ability to limit unauthorized access and manipulation, that input and output of data are processed correctly on the system, that any changes to the system are authorized, and that users have access to the system.

Licensed to Berend Post berend.post@it-university.nl

Question 672

Organization A has a Software as a Service Agreement (SaaS) with Organization B. The software is vital to Organization A. Which of the following would provide the GREATEST assurance that the application can be recovered in the event of a disaster?

- ☐ Organization B is responsible for disaster recovery and held accountable for interruption of service.
- ☐ Organization A has a source code escrow agreement and hardware procurement provisions for disaster recovery purposes.
- ☒ Organization B has a disaster recovery plan included in its contract and allows oversight by Organization A.
- ☐ Organization A buys disaster insurance to recuperate losses in the event of a disaster.

Question 673

Which of the following attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☒ Interrupt attack

Explanation:

An Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Example: A boot sector virus typically issues an interrupt to execute a write to the boot sector.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Licensed to Berend Post berend.post@it-university.nl

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cyber crime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 322

Question 674

Which of the following is the MAIN purpose of data classification?

- ☒ Applying the appropriate protective measures
- ☐ Ensuring the segregation of duties
- ☐ Defining requirements of security labels
- ☐ Ensuring integrity of sensitive information

Question 675

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

- ☐ ask the auditee to sign a release form accepting full legal responsibility.
- ☒ elaborate on the significance of the finding and the risks of not correcting it.
- ☐ report the disagreement to the audit committee for resolution.
- ☐ accept the auditee's position since they are the process owners.

Explanation:

Explanation:

If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

Licensed to Berend Post berend.post@it-university.nl

Question 676

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

- ☐ test the software for compatibility with existing hardware.
- ☐ perform a gap analysis.
- ☐ review the licensing policy.
- ☒ ensure that the procedure had been approved.

Explanation:

Explanation:

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

Question 677

Which of the following would be the MOST significant audit finding when reviewing a point-of-sale (POS) system?

- ☐ invoices recorded on the POS system are manually entered into an accounting application
- ☐ An optical scanner is not used to read bar codes for the generation of sales invoices
- ☐ Frequent power outages occur, resulting in the manual preparation of invoices
- ☒ Customer credit card information is stored unencrypted on the local POS system

Explanation:

Explanation:

It is important for the IS auditor to determine if any credit card information is stored on the local point-of-sale (POS) system. Any such information, if stored, should be encrypted or protected by other means to avoid the possibility of unauthorized disclosure. Manually inputting sale invoices into the accounting application is an operational issue, if the POS system were to be interfaced with the financial accounting application, the overall efficiency could be improved. The nonavailability of optical scanners to read bar codes of the products and power outages are operational issues.

Licensed to Berend Post berend.post@it-university.nl

Question 678

The MOST appropriate person to chair the steering committee for an enterprise-wide system development should normally be the:

- ☐ project manager
- ☐ IS director
- ☒ executive level manager.
- ☐ business analyst

Question 679

An IS auditor finds multiple situations where the help desk resolved security incidents without notifying IT security as required by policy. Which of the following is the BEST audit recommendation?

- ☐ Display the incident response hotline in common areas.
- ☒ Have IT security review problem management policy.
- ☐ Reinforce the incident escalation process.
- ☐ Redesign the help desk reporting process.

Question 680

An IS auditor reviewing access controls for a client-server environment should FIRST:

- ☐ evaluate the encryption technique.
- ☒ identify the network access points.
- ☐ review the identity management system.
- ☐ review the application level access controls.

Explanation:

Explanation:

A client-server environment typically contains several access points and utilizes distributed techniques, increasing the risk of unauthorized access to data and processing. To evaluate the security of the client server environment, all network access points should be identified. Evaluating encryption techniques, reviewing the identity management system and reviewing the application level access controls would be performed at a later stage of the review.

Licensed to Berend Post berend.post@it-university.nl

Question 681

Which of the following statement correctly describes the differences between tunnel mode and transport mode of the IPSec protocol?

- ☒ In transport mode the ESP is encrypted where as in tunnel mode the ESP and its header's are encrypted
- ☐ In tunnel mode the ESP is encrypted where as in transport mode the ESP and its header's are encrypted
- ☐ In both modes (tunnel and transport mode) the ESP and its header's are encrypted
- ☐ There is no encryption provided when using ESP or AH

Explanation:

ESP can be used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology. For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.

In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

 Licensed to Berend Post berend.post@it-university.nl

The other options presented are invalid as the transport mode encrypts ESP and the tunnel mode encrypts ESP and its header's.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 353

Question 682

The PRIMARY benefit of using secure shell (SSH) to access a server on a network is that it:

- ☐ provides better session reliability.
- ☐ prevents man-in-the-middle attacks.
- ☒ provides confidentiality of transmitted data.
- ☐ facilitates communication across platforms.

Question 683

Which of the following is a function of an IS steering committee?

- ☐ Monitoring vendor-controlled change control and testing
- ☐ Ensuring a separation of duties within the information's processing environment
- ☒ Approving and monitoring major projects, the status of IS plans and budgets
- ☐ Liaising between the IS department and the end users

Explanation:

Explanation:

The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

Question 684

What is the most common reason for information systems to fail to meet the needs of users?

- ☐ Lack of funding
- ☒ Inadequate user participation during system requirements definition
- ☐ Inadequate senior management participation during system requirements definition
- ☐ Poor IT strategic planning

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Inadequate user participation during system requirements definition is the most common reason for information systems to fail to meet the needs of users.

Question 685

An organization is choosing key performance indicators (KPIs) for its information security management. Which of the following KPIs would provide stakeholders with the MOST useful information about whether information security risk is being managed?

- ☐ Time from initial reporting of an incident to appropriate escalation
- ☒ Time from identifying a security threat to implementing a solution
- ☐ The number of security controls implemented
- ☐ The number of security incidents during the past quarter

Question 686

Which of the following provides the GREATEST assurance that any confidential information on a disk is no longer accessible but the device is still usable by other internal users?

- ☒ Reformatting the disk
- ☐ Erasing the disk
- ☐ Degaussing the disk
- ☐ Password-protecting the disk

Question 687

Which of the following types of firewall treats each network frame or packet in isolation?

- ☐ statefull firewall
- ☐ hardware firewall
- ☐ combination firewall
- ☐ packet filtering firewall
- ☒ stateless firewall
- ☐ None of the choices.

Explanation:

Explanation:

A stateless firewall treats each network frame or packet in isolation.

Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

Licensed to Berend Post berend.post@it-university.nl

Question 688

An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

- ☐ maintenance of access logs of usage of various system resources.
- ☒ authorization and authentication of the user prior to granting access to system resources.
- ☐ adequate protection of stored data on servers by encryption or other means.
- ☐ accountability system and the ability to identify any terminal accessing system resources.

Explanation:

Explanation:

The authorization and authentication of users is the most significant aspect in a telecommunications access control review, as it is a preventive control. Weak controls at this level can affect all other aspects. The maintenance of access logs of usage of system resources is a detective control. The adequate protection of data being transmitted to and from servers by encryption or other means is a method of protecting information during transmission and is not an access issue. The accountability system and the ability to identify any terminal accessing system resources deal with controlling access through the identification of a terminal.

Question 689

An internal control audit has revealed a control deficiency related to a legacy system where the compensating controls no longer appear to be effective. Which of the following would BEST help the information security manager determine the security requirements to resolve the control deficiency?

- ☐ Cost-benefit analysis
- ☒ Gap analysis
- ☐ Risk assessment
- ☐ Business case

Question 690

Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

- ☐ Pilot
- ☒ Paper
- ☐ Unit
- ☐ System

Explanation:

Explanation:

A paper test is appropriate for testing a BCP. it is a walkthrough of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster. Choices A, C and D are not appropriate for a BCP.

Licensed to Berend Post berend.post@it-university.nl

Question 691

Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

- ☐ Registration authority
- ☒ Certificate authority (CA)
- ☐ Certification relocation list
- ☐ Certification practice statement

Explanation:

Explanation:

The certificate authority maintains a directory of digital certificates for the reference of those receiving them, it manages the certificate life cycle, including certificate directory maintenance and certificate revocation list maintenance and publication. Choice A is not correct because a registration authority is an optional entity that is responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA. Choice C is incorrect since a CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. Choice D is incorrect because a certification practice statement is a detailed set of rules governing the certificate authority's operations.

Question 692

A government organization uses standard Wi-Fi Protected Access 2 (WPA2) to protect confidential information transmitted to a file server. Which of the following is the IS auditor's BEST recommendation to further strengthen security?

- ☐ Certificate-based authentication
- ☐ Network address translation (NAT)
- ☐ Media access control (MAC) address filtering
- ☒ Service set identifier (SSID) masking

Question 693

The GREATEST advantage of using web services for the exchange of information between two systems is:

- ☐ secure communications.
- ☐ improved performance.
- ☒ efficient interfacing.
- ☐ enhanced documentation.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

Question 694

Which of the following would be the BEST performance indicator for the effectiveness of an incident management program?

- ☐ Incident alert meantime
- ☐ Average time between incidents
- ☒ Number of incidents reported
- ☐ Incident resolution meantime

Question 695

Which of the following is the INCORRECT “layer - protocol" mapping within the TCP/IP model?

- ☐ Application layer – NFS
- ☐ Transport layer – TCP
- ☒ Network layer – UDP
- ☐ LAN or WAN interface layer – point-to-point protocol

Explanation:

The word INCORRECT is the keyword used in the question.

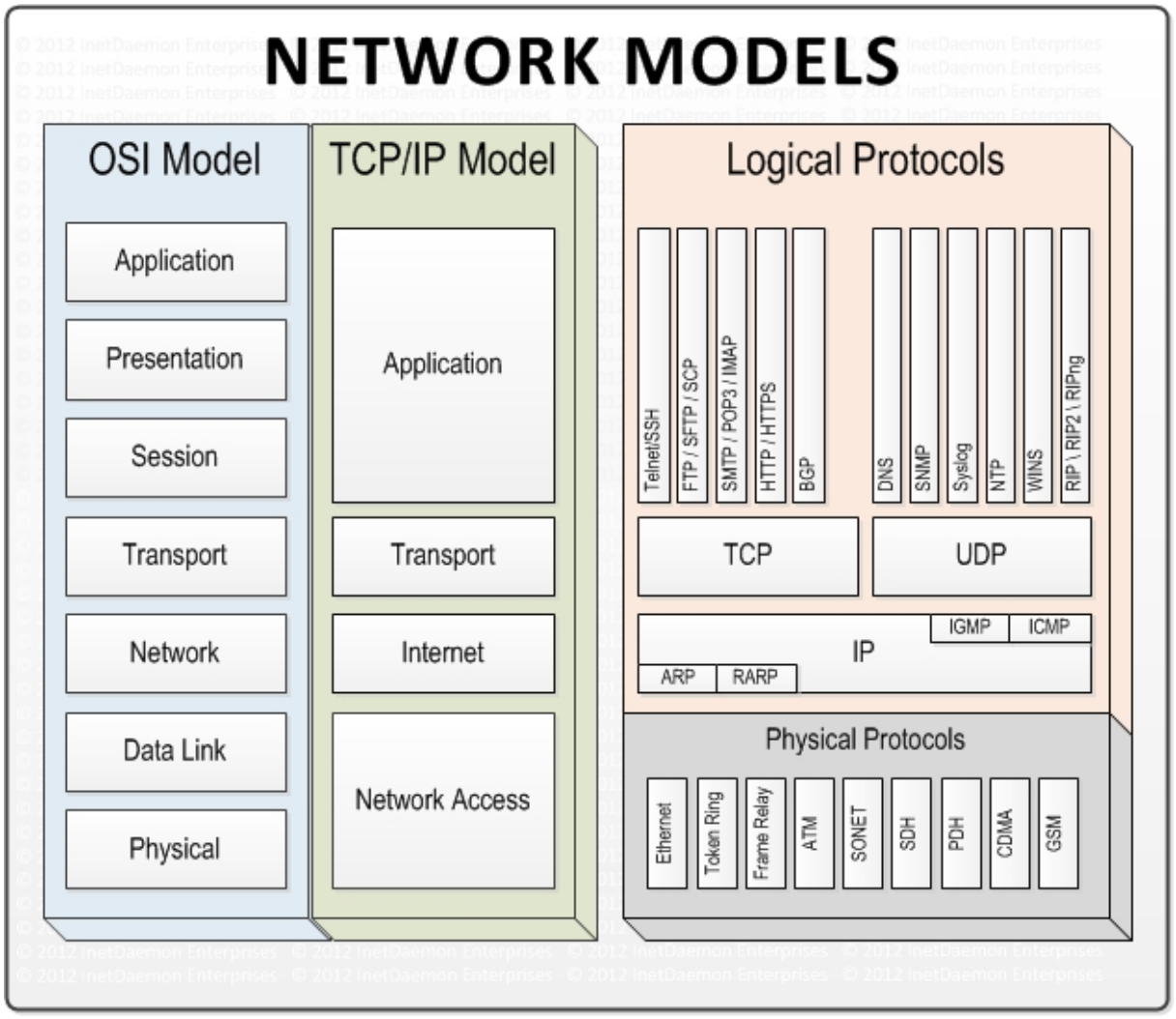
You need to find out invalid layer-protocol mapping.

The UDP protocol works at Transport layer of a TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

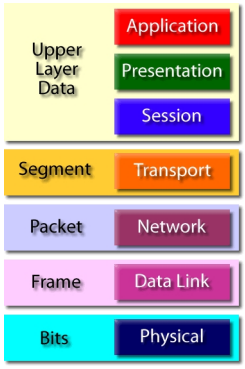
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe layer-protocol mapping in TCP/IP protocol.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 696

Which of the following would impair the independence of a quality assurance team?

- ☐ Ensuring compliance with development methods
- ☐ Checking the testing assumptions
- ☒ Correcting coding errors during the testing process
- ☐ Checking the code to ensure proper documentation

Explanation:

Explanation:

Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.

Licensed to Berend Post berend.post@it-university.nl

Question 697

Which of the following is MOST important when evaluating the retention period for a cloud provider's client data backups?

- ☐ Cost of data storage
- ☒ Contractual commitments
- ☐ Previous audit recommendations
- ☐ Industry best practice

Question 698

Which of the following provides the MOST assurance that a newly developed web application does not have IT security issues?

- ☐ Server hardening
- ☐ Business impact analysis (BIA)
- ☐ Application whitelisting
- ☒ Penetration testing

Question 699

Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of integrity?

- ☐ Ensuring encryption for data in transit
- ☐ Implementing a data classification schema
- ☒ Utilizing a formal change management process
- ☐ Enforcing service level agreements (SLAs)

Question 700

One advantage of managing an entire collection of projects as a portfolio is that it highlights the need to:

- ☐ identify dependencies between projects.
- ☐ inform users about all ongoing projects.
- ☐ manage the risk of each individual project.
- ☒ manage the quality of each project.

Licensed to Berend Post berend.post@it-university.nl

Question 701

Which of the following cloud deployment model is provisioned for open use by the general public?

- ☐ Private Cloud
- ☐ Community Cloud
- ☒ Public Cloud
- ☐ Hybrid Cloud

Explanation:

In Public cloud, the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

For your exam you should know below information about Cloud Computing deployment models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

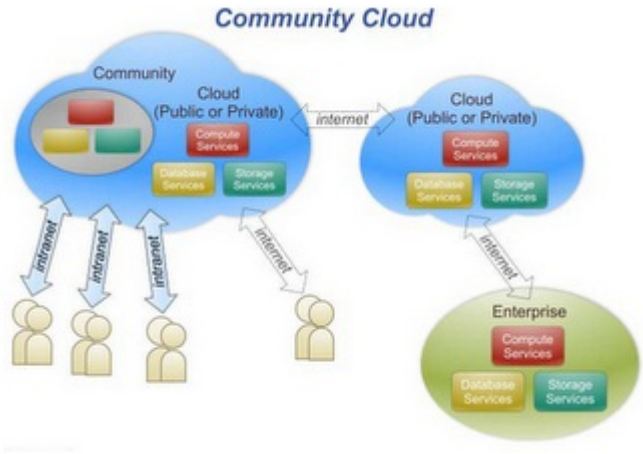
Private Cloud

Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud

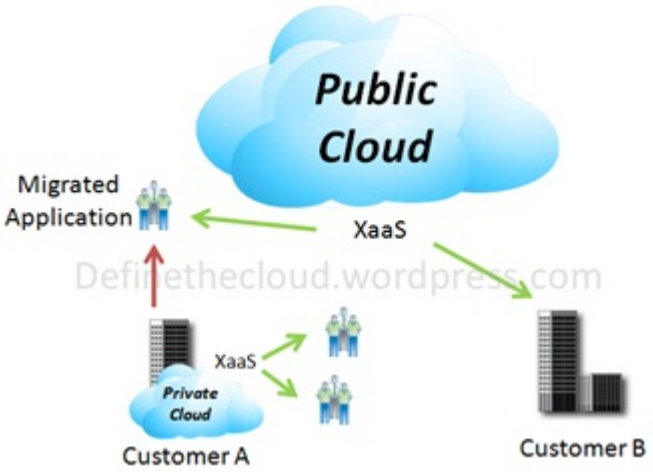
Licensed to Berend Post berend.post@it-university.nl



Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Public Cloud

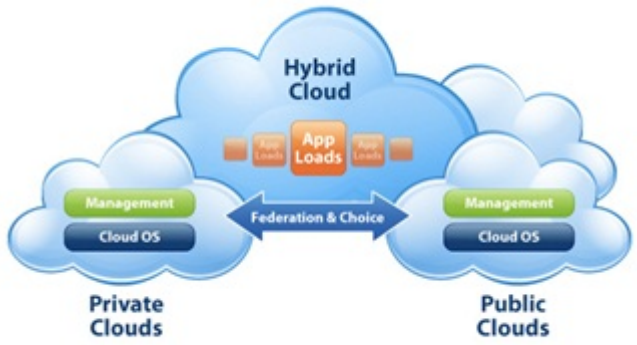


Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

hybrid cloud

Licensed to Berend Post berend.post@it-university.nl



The following answers are incorrect:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

Licensed to Berend Post berend.post@it-university.nl

Question 702

Which of the following is the BEST time for an IS auditor to perform a post-implementation review?

- ☒ When the system has stabilized.
- ☐ After the completion of user testing.
- ☐ Before decommissioning the legacy system.
- ☐ Immediately after the new system goes into production.

Question 703

Which of the following is a tool you can use to simulate a big network structure on a single computer?

- ☐ honeymoon
- ☐ honeytrap
- ☐ honeytube
- ☒ honeyd
- ☐ None of the choices.

Explanation:

Explanation:

honeyd is a GPL licensed software you can use to simulate a big network structure on a single computer.

Question 704

An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

- ☐ alignment of the BCP with industry best practices.
- ☒ results of business continuity tests performed by IS and end-user personnel.
- ☐ off-site facility, its contents, security and environmental controls.
- ☐ annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Explanation:

Explanation:

The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

Licensed to Berend Post berend.post@it-university.nl

Question 705

The lack of which of the following represents the GREATEST risk to the quality of developed software?

- ☐ Code reviews
- ☐ Periodic internal audits
- ☐ Load testing
- ☒ An enterprise architecture

Question 706

When an organization and its IT-hosting service provider are establishing a contract with each other, it is MOST important that the contract includes:

- ☒ each party's security responsibilities
- ☐ details of expected security metrics
- ☐ penalties for noncompliance with security policy
- ☐ recovery time objectives (RTOs)

Question 707

Which of the following network configuration options contains a direct link between any two host machines?

- ☐ Bus
- ☐ Ring
- ☐ Star
- ☒ Completely connected (mesh)

Explanation:

Explanation:

A completely connected mesh configuration creates a direct link between any two host machines.

Question 708

Which of the following features can be provided only by asymmetric encryption?

- ☐ 128-bit key length
- ☐ Information privacy
- ☐ Data confidentiality
- ☒ Nonrepudiation

Licensed to Berend Post berend.post@it-university.nl

Question 709

A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?

- ☒ Audit logs are not enabled for the system
- ☐ A logon ID for the technical lead still exists
- ☐ Spyware is installed on the system
- ☐ A Trojan is installed on the system

Explanation:

Explanation:

Audit logs are critical to the investigation of the event; however, if not enabled, misuse of the logon ID of the technical lead and the guest account could not be established. The logon ID of the technical lead should have been deleted as soon as the employee left the organization but, without audit logs, misuse of the ID is difficult to prove. Spyware installed on the system is a concern but could have been installed by any user and, again, without the presence of logs, discovering who installed the spyware is difficult. A Trojan installed on the system is a concern, but it can be done by any user as it is accessible to the whole group and, without the presence of logs, investigation would be difficult.

Question 710

Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery, in such an environment, it is essential that:

- ☒ each plan is consistent with one another.
- ☐ all plans are integrated into a single plan.
- ☐ each plan is dependent on one another.
- ☐ the sequence for implementation of all plans is defined.

Explanation:

Explanation:

Depending on the complexity of an organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan. However, each plan has to be consistent with other plans to have a viable business continuity planning strategy. It may not be possible to define a sequence in which plans have to be implemented, as it may be dependent on the nature of disaster, criticality, recovery time, etc.

Licensed to Berend Post berend.post@it-university.nl

Question 711

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

- ☐ rely on senior management to enforce security
- ☒ promote the relevance and contribution of security
- ☐ reiterate the necessity of security
- ☐ focus on compliance

Question 712

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

- ☐ Nonconnection-oriented protocols
- ☒ Connection-oriented protocols
- ☐ Session-oriented protocols
- ☐ Nonsession-oriented protocols

Explanation:

Explanation:

The transport layer of the TCP/IP protocol suite provides for connection- oriented protocols to ensure reliable communication.

Question 713

After threats to a data center are identified, an IS auditor would expect management to FIRST:

- ☐ recommend required actions to executive management.
- ☐ discuss risk management practices with neighboring firms.
- ☒ implement procedures to address all identified threats.
- ☐ establish and quantify the potential effects if each threat occurs.

Question 714

The PRIMARY focus of a training curriculum for members of an incident response team should be:

- ☐ technology training.
- ☐ security awareness.
- ☐ external corporate communication.
- ☒ specific role training.

Licensed to Berend Post berend.post@it-university.nl

Question 715

Which of the following audit risk is related to exposure of a process or entity to be audited without taking into account the control that management has implemented?

- ☒ Inherent Risk
- ☐ Control Risk
- ☐ Detection Risk
- ☐ Overall Audit Risk

Explanation:

Explanation:

Inherent Risk is the risk level or exposure of a process or entity to be audited without taking into account the control that management has implemented. Inherent risk exists independent of an audit and can occur because of the nature of the business.

For your exam you should know below information about audit risk:

Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR), and can be calculated thus:

AR = IR • CR • DR

Inherent Risk

Auditors must determine risks when working with clients. One type of risk to be aware of is inherent risk. While assessing this level of risk, you ignore whether the client has internal controls in place (such as a secondary review of financial statements) in order to help mitigate the inherent risk. You consider the strength of the internal controls when assessing the client's control risk. Your job when assessing inherent risk is to evaluate how susceptible the financial statement assertions are to material misstatement given the nature of the client's business. A few key factors can increase inherent risk.

Environment and external factors: Here are some examples of environment and external factors that can lead to high inherent risk:

Rapid change: A business whose inventory becomes obsolete quickly experiences high inherent risk.

Licensed to Berend Post berend.post@it-university.nl

Expiring patents: Any business in the pharmaceutical industry also has inherently risky environment and external factors. Drug patents eventually expire, which means the company faces competition from other manufacturers marketing the same drug under a generic label.

State of the economy: The general level of economic growth is another external factor affecting all businesses.

Availability of financing: Another external factor is interest rates and the associated availability of financing. If your client is having problems meeting its short-term cash payments, available loans with low interest rates may mean the difference between your client staying in business or having to close its doors.

Prior-period misstatements: If a company has made mistakes in prior years that weren't material (meaning they weren't significant enough to have to change), those errors still exist in the financial statements. You have to aggregate prior-period misstatements with current year misstatements to see if you need to ask the client to adjust the account for the total misstatement.

You may think an understatement in one year compensates for an overstatement in another year. In auditing, this assumption isn't true. Say you work a cash register and one night the register comes up $20 short. The next week, you somehow came up $20 over my draw count. The $20 differences are added together to represent the total amount of your mistakes which is $40 and not zero. Zero would indicate no mistakes at all had occurred.

Susceptibility to theft or fraud: If a certain asset is susceptible to theft or fraud, the account or balance level may be considered inherently risky. For example, if a client has a lot of customers who pay in cash, the balance sheet cash account is going to have risk associated with theft or fraud because of the fact that cash is more easily diverted than customer checks or credit card payments.

Looking at industry statistics relating to inventory theft, you may also decide to consider the inventory account as inherently risky. Small inventory items can further increase the risk of this account valuation being incorrect because those items are easier to conceal (and therefore easier to steal).

Control Risk

Control risk has been defined under International Standards of Auditing (ISAs) as following:

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control.

Licensed to Berend Post berend.post@it-university.nl

In simple words control risk is the probability that a material misstatement exists in an assertion because that misstatement was not either prevented from entering entity's financial information or it was not detected and corrected by the internal control system of the entity.

It is the responsibility of the management and those charged with governance to implement internal control system and maintain it appropriately which includes managing control risk.

There can be many reasons for control risk to arise and why it cannot be eliminated absolutely. But some of them are as follows:

Cost-benefit constraints

Circumvention of controls

Inappropriate design of controls

Inappropriate application of controls

Lack of control environment and accountability

Novel situations

Outdated controls

Inappropriate segregation of duties

Detection Risk

Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements.

An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions.

Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

The following answers are incorrect:

Control Risk - The risk that material error exist that would not be prevented or detected on timely basis by the system of internal controls.

Licensed to Berend Post berend.post@it-university.nl

Detection risk - The risk that material errors or misstatements that have occurred will not be detected by an IS auditor.

Overall audit risk - The probability that information or financial report may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under security so the overall audit risk is at sufficiently low level at the completion of the examination.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 50

http://en.wikipedia.org/wiki/Audit_risk

http://www.dummies.com/how-to/content/how-to-assess-inherent-risk-in-an-audit.html

http://pakaccountants.com/what-is-control-risk/

http://accounting-simplified.com/audit/risk-assessment/audit-risk.html

Question 716

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?

- ☐ CRC-32
- ☐ CRC-64
- ☐ DES
- ☐ 3DES
- ☒ RC4
- ☐ RC5
- ☐ None of the choices.

Explanation:

Explanation:

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

Licensed to Berend Post berend.post@it-university.nl

Question 717

An IS auditor is assigned to perform a post implementation review of an application system. Which pf the following situations may have impaired the independence of the IS auditor? The IS auditor:

- ☒ implemented a specific control during the development of the application system.
- ☐ designed an embedded audit module exclusively for auditing the application system.
- ☐ participated as a member of the application system project team, but did not have operational responsibilities.
- ☐ provided consulting advice concerning application system best practices.

Explanation:

Explanation:

Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair an IS auditor's independence. Choice D is incorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

Question 718

An IT management group has developed a standardized security control checklist and distributed it to the control self-assessors in each organizational unit. Which of the following is the GREATEST risk in this approach?

- ☐ Delayed feedback may increase exposures
- ☐ Over time the checklist may become outdated
- ☒ Assessors may manipulate the results
- ☐ Business-specific vulnerabilities may be overlooked

Question 719

An IS auditor identifies key controls that have been overridden by management. The NEXT step the IS auditor should take is to:

- ☐ perform procedures to quantify the irregularities.
- ☒ report the absence of key controls to regulators.
- ☐ recommend compensating controls.
- ☐ withdraw from the engagement.

Licensed to Berend Post berend.post@it-university.nl

Question 720

Which of the following statement is NOT true about smoke detector?

- ☐ The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
- ☐ The smoke detector should produce an audible alarm when activated and be linked to a monitored station
- ☐ The location of the smoke detector should be marked on the tiling for easy identification and access
- ☒ Smoke detector should replace fire suppression system

Explanation:

The word NOT is the keyword used in the question. You need to find out a statement which is not applicable to smoke detector. Smoke detector should supplement, not replace, fire suppression system.

For CISA exam you should know below information about smoke detector.

The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor.

The smoke detector should produce an audible alarm when activated be linked to a monitored station

The location of the smoke detector should be marked on the tiling for easy identification and access.

Smoke detector should supplement, not replace, fire suppression system

The following were incorrect answers:

The other presented options are valid statement about smoke detector.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number373

Licensed to Berend Post berend.post@it-university.nl

Question 721

When engaging services from external auditors, which of the following should be established FIRST?

- ☐ Termination conditions agreements
- ☒ Nondisclosure agreements
- ☐ Service level agreements
- ☐ Operational level agreements

Question 722

Which are the two primary types of scanner used for protecting against Malware?

- ☒ Malware mask/signatures and Heuristic Scanner
- ☐ Active and passive Scanner
- ☐ Behavioral Blockers and immunizer Scanner
- ☐ None of the above

Explanation:

Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

For CISA exam you should know below mentioned different kinds of malware Controls

A. Active Monitors - Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Licensed to Berend Post berend.post@it-university.nl

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other types of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker - Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

The following were incorrect answers:

The other options presented are not a valid primary types of scanner.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 354 and 355

Question 723

Disaster recovery planning (DRP) addresses the:

- ☒ technological aspect of business continuity planning.
- ☐ operational piece of business continuity planning.
- ☐ functional aspect of business continuity planning.
- ☐ overall coordination of business continuity planning.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Disaster recovery planning (DRP) is the technological aspect of business continuity planning. Business resumption planning addresses the operational part of business continuity planning.

Question 724

There is a concern that a salesperson may download an organization's full customer list from the Software as a Service (SaaS) when leaving to work for a competitor. Which of the following would BEST help to identify this type of incident?

- ☒ Monitor applications logs
- ☐ Disable remote access to the application
- ☐ Implement a web application firewall
- ☐ Implement an intrusion detection system (IDS)

Question 725

Which of the following activities should occur after a business impact analysis (BIA)?

- ☐ Identify threats to the IT environment
- ☐ Identify critical applications
- ☒ Analyze recovery options
- ☐ Review the computing and user environment

Question 726

What would be the MOST effective control for enforcing accountability among database users accessing sensitive information?

- ☒ implement a log management process
- ☐ implement a two-factor authentication
- ☐ Use table views to access sensitive data
- ☐ Separate database and application servers

Explanation:

Explanation:

Accountability means knowing what is being done by whom. The best way to enforce the principle is to implement a log management process that would create and store logs with pertinent information such as user name, type of transaction and hour. Choice B, implementing a two- factor authentication, and choice C, using table views to access sensitive data, are controls that would limit access to the database to authorized users but would not resolve the accountability problem. Choice D may help in a better administration or even in implementing access controls but, again, does not address the accountability issues.

Licensed to Berend Post berend.post@it-university.nl

Question 727

Which of the following kinds of function are particularly vulnerable to format string attacks?

- ☒ C functions that perform output formatting
- ☐ C functions that perform integer computation
- ☐ C functions that perform real number subtraction
- ☐ VB functions that perform integer conversion
- ☐ SQL functions that perform string conversion
- ☐ SQL functions that perform text conversion

Explanation:

Explanation:

Format string attacks are a new class of vulnerabilities recently discovered. It can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as print (). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token.

Question 728

Which of the following BEST limits the impact of server failures in a distributed environment?

- ☐ Redundant pathways
- ☒ Clustering
- ☐ Dial backup lines
- ☐ Standby power

Explanation:

Explanation:

Clustering allows two or more servers to work as a unit, so that when one of them fails, the other takes over. Choices A and C are intended to minimize the impact of channel communications failures, but not a server failure. Choice D provides an alternative power source in the event of an energy failure.

Question 729

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

- ☐ With public-key encryption, or symmetric encryption
- ☒ With public-key encryption, or asymmetric encryption
- ☐ With shared-key encryption, or symmetric encryption
- ☐ With shared-key encryption, or asymmetric encryption

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

Question 730

When is the BEST time to commence continuity planning for a new application system?

- ☐ Immediately after implementation
- ☐ Just prior to the handover to the system maintenance group
- ☒ During the design phase
- ☐ Following successful user testing

Question 731

Which of the following is the MOST important outcome of testing incident response plans?

- ☒ Internal procedures are improved.
- ☐ An action plan is available for senior management.
- ☐ Staff is educated about current threats.
- ☐ Areas requiring investment are identified.

Question 732

When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☒ The point at which controls are exercised as data flow through the system
- ☐ Only preventive and detective controls are relevant
- ☐ Corrective controls can only be regarded as compensating
- ☐ Classification allows an IS auditor to determine which controls are missing

Explanation:

Explanation:

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect, since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

Licensed to Berend Post berend.post@it-university.nl

Question 733

Which of the following goals would you expect to find in an organization's strategic plan?

- ☐ Test a new accounting package.
- ☐ Perform an evaluation of information technology needs.
- ☐ Implement a new project planning system within the next 12 months.
- ☒ Become the supplier of choice for the product offered.

Explanation:

Explanation:

Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

Question 734

An IS auditor discovered abnormalities in a monthly report generated from a system upgraded six months ago. Which of the following should be the auditor's FIRST course of action?

- ☐ Inspect source code for proof of abnormalities
- ☐ Perform a change management review of the system
- ☐ Schedule an access review of the system
- ☒ Determine the impact of abnormalities in the report

Question 735

When developing an escalation process for an incident response plan, the information security manager should PRIMARLY consider the:

- ☐ affected stakeholders
- ☐ availability of technical resources
- ☒ incident response team
- ☐ media coverage

Licensed to Berend Post berend.post@it-university.nl

Question 736

Which of the following is the MOSTlikely reason an organization would use Platform as a Service (PaaS)?

- ☐ To operate third-party hosted applications
- ☐ To install and manage operating systems
- ☐ To establish a network and security architecture
- ☒ To develop and integrate its applications

Question 737

Which of the following cloud deployment model can be shared by several organizations?

- ☐ Private Cloud\
- ☒ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Explanation:

In Community cloud, the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

For your exam you should know below information about Cloud Computing deployment models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

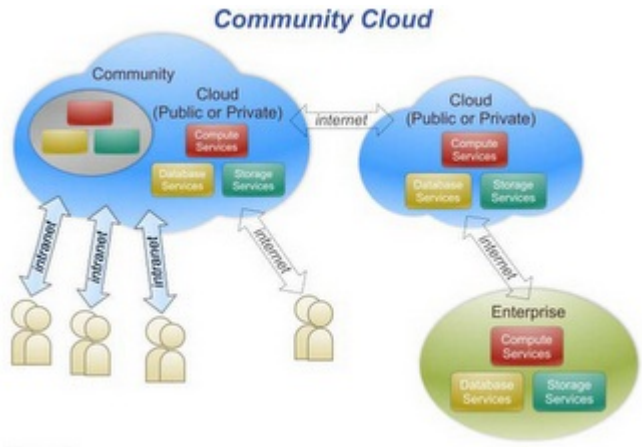
Private Cloud

Licensed to Berend Post berend.post@it-university.nl

Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud

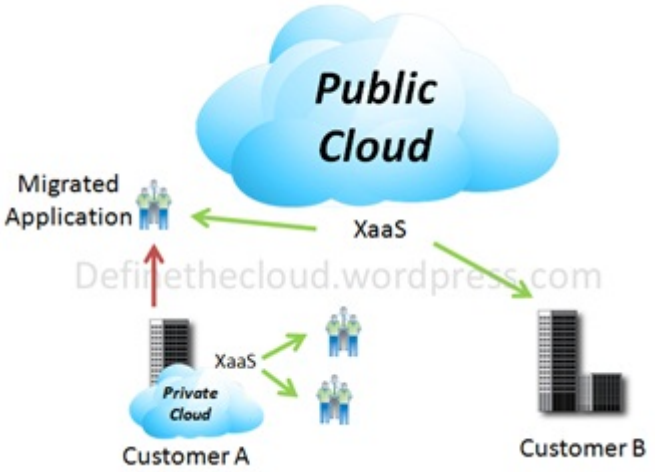


Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Public Cloud

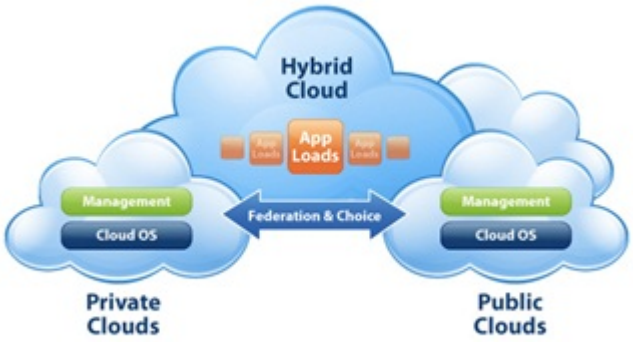
Licensed to Berend Post berend.post@it-university.nl



Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

hybrid cloud



The following answers are incorrect:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Licensed to Berend Post berend.post@it-university.nl

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

Question 738

The maturity level of an organization's problem management support function is optimized when the function:

- ☒ proactively provides solutions
- ☐ has formally documented the escalation process
- ☐ analyzes critical incidents to identify root cause
- ☐ resolves requests in a timely manner

Question 739

Which of the following is the BEST way to facilitate proper follow-up for audit findings?

- ☐ Schedule a follow-up audit for two weeks after the initial audit was completed.
- ☐ Conduct a surprise audit to determine whether remediation is in progress.
- ☐ Conduct a follow-up audit when findings escalate to incidents.
- ☒ Schedule a follow-up audit based on remediation due dates.

Question 740

Applying a retention date on a file will ensure that:

- ☐ data cannot be read until the date is set.
- ☒ data will not be deleted before that date.
- ☐ backup copies are not retained after that date.
- ☐ datasets having the same name are differentiated.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

Question 741

Which of the following system and data conversion strategies provides the GREATEST redundancy?

- ☐ Direct cutover
- ☐ Pilot study
- ☐ Phased approach
- ☒ Parallel run

Explanation:

Explanation:

Parallel runs are the safest-though the most expensive-approach, because both the old and new systems are run, thus incurring what might appear to be double costs. Direct cutover is actually quite risky, since it does not provide for a 'shake down period' nor does it provide an easy fallback option. Both a pilot study and a phased approach are performed incrementally, making rollback procedures difficult to execute.

Question 742

Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☒ Jitter

Explanation:

Simply said, the time difference in packet inter-arrival time to their destination can be called jitter. Jitter is specific issue that normally exists in packet switched networks and this phenomenon is usually not causing any communication problems. TCP/IP is responsible for dealing with the jitter impact on communication.

On the other hand, in VoIP network environment, or better say in any bigger environment today where we use IP phones on our network this can be a bigger problem. When someone is sending VoIP communication at a normal interval (let's say one frame every 10 ms) those packets can stuck somewhere in between inside the packet network and not arrive at expected regular peace to the destined station. That's the whole jitter phenomenon all about so we can say that the anomaly in tempo with which packet is expected and when it is in reality received is jitter.

Licensed to Berend Post berend.post@it-university.nl

jitter

In this image above, you can notice that the time it takes for packets to be send is not the same as the period in which the will arrive on the receiver side. One of the packets encounters some delay on his way and it is received little later than it was asumed. Here are the jitter buffers entering the story. They will mitigate packet delay if required. VoIP packets in networks have very changeable packet inter-arrival intervals because they are usually smaller than normal data packets and are therefore more numerous with bigger chance to get some delay along the way.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Licensed to Berend Post berend.post@it-university.nl

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 275

and

http://howdoesinternetwork.com/2013/jitter

Question 743

A new information security manager is charged with reviewing and revising the information security strategy. The information security manager's FIRST course of action should be to gain an understanding of the organization's:

- ☐ security architecture
- ☐ risk register
- ☐ internal control framework
- ☒ business strategy

Licensed to Berend Post berend.post@it-university.nl

Question 744

When preparing an audit report, the IS auditor should ensure that the results are supported by:

- ☐ statements from IS management.
- ☐ workpapers of other auditors.
- ☐ an organizational control self-assessment.
- ☒ sufficient and appropriate audit evidence.

Explanation:

Explanation:

ISACA's standard on 'reporting' requires the IS auditor have sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence collected during the course of the review even though the auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment (CSA) could supplement the audit findings. Choices A, B and C might be referenced during an audit but, of themselves, would not be considered a sufficient basis for issuing a report.

Question 745

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

- ☒ Power line conditioners
- ☐ Surge protective devices
- ☐ Alternative power supplies
- ☐ Interruptible power supplies

Explanation:

Explanation:

Power line conditioners are used to compensate for peaks and valleys in the power supply and reduce peaks in the power flow to what is needed by the machine. Any valleys are removed by power stored in the equipment. Surge protection devices protect against high- voltage bursts. Alternative power supplies are intended for computer equipment running for longer periods and are normally coupled with other devices such as an uninterruptible power supply (UPS) to compensate for the power loss until the alternate power supply becomes available. An interruptible power supply would cause the equipment to come down whenever there was a power failure.

Licensed to Berend Post berend.post@it-university.nl

Question 746

Which of the following is of greatest concern when performing an IS audit?

- ☒ Users' ability to directly modify the database
- ☐ Users' ability to submit queries to the database
- ☐ Users' ability to indirectly modify the database
- ☐ Users' ability to directly view the database

Explanation:

Explanation:

A major IS audit concern is users' ability to directly modify the database.

Question 747

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- ☐ control self-assessments.
- ☐ a business impact analysis.
- ☒ an IT balanced scorecard.
- ☐ business process reengineering.

Explanation:

Explanation:

An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. Control self- assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

Question 748

Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?

- ☐ Degaussing
- ☐ Defragmenting
- ☐ Erasing
- ☒ Destroying

Explanation:

Explanation:

Destroying magnetic media is the only way to assure that confidential information cannot be recovered. Degaussing or demagnetizing is not sufficient to fully erase information from magnetic media. The purpose of defragmentation is to eliminate fragmentation in file systems and does not

Licensed to Berend Post berend.post@it-university.nl

remove information. Erasing or deleting magnetic media does not remove the information; this method simply changes a file's indexing information.

Question 749

A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value can be mitigated by:

- ☐ requiring the recipient to use a different hash algorithm.
- ☐ generating hash output that is the same size as the original message.
- ☒ using a secret key in conjunction with the hash algorithm.
- ☐ using the sender’s public key to encrypt the message.

Question 750

Which of the following BEST supports the risk assessment process to determine criticality of an asset?

- ☐ Threat assessment
- ☐ Residual risk analysis
- ☐ Vulnerability assessment
- ☒ Business impact analysis (BIA)

Question 751

The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- ☐ the target's management hands-on involvement.
- ☐ the target's location.
- ☒ the target's size and complexity.
- ☐ the target's budget.
- ☐ the target's head count.
- ☐ None of the choices.

Explanation:

Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

Licensed to Berend Post berend.post@it-university.nl

Question 752

An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

- ☐ The new access points with stronger security are affordable.
- ☐ The old access points are poorer in terms of performance.
- ☒ The organization's security would be as strong as its weakest points.
- ☐ The new access points are easier to manage.

Explanation:

Explanation:

The old access points should be discarded and replaced with products having strong security; otherwise, they will leave security holes open for attackers and thus make the entire network as weak as they are. Affordability is not the auditor's major concern. Performance is not as important as security in this situation. Product manageability is not the IS auditor's concern.

Question 753

Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

- ☒ buffer overflow
- ☐ format string vulnerabilities
- ☐ integer misappropriation
- ☐ code injection
- ☐ None of the choices.

Explanation:

Explanation:

A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

Question 754

What is a callback system?

- ☐ It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fails.
- ☐ It is a remote-access system whereby the user's application automatically redials the remote access server if the initial connection attempt fails.
- ☒ It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server,

Licensed to Berend Post berend.post@it-university.nl

which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

☐ It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of time.

Explanation:

Explanation:

A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

Question 755

Rather than decommission an entire legacy application, an organization's IT department has chosen to replace specific modules while maintaining those still relevant. Which of the following artifacts is MOST important for an IS auditor to review?

☐ IT service management catalog and service level requirements
☐ Security requirements for legacy data masking and data destruction
☐ Applicable licensing agreements for the application
☒ Future state architecture and requirements

Question 756

Integer overflow occurs primarily with:

☐ string formatting
☐ debug operations
☐ output formatting
☐ input verifications
☒ arithmetic operations
☐ None of the choices.

Explanation:

Explanation:

An integer overflow occurs when an arithmetic operation attempts to create a numeric value that is larger than can be represented within the available storage space. On some processors the result saturates - once the maximum value is reached attempts to make it larger simply return the maximum result.

Licensed to Berend Post berend.post@it-university.nl

Question 757

Which of the following function in traditional EDI process manipulates and routes data between the application system and the communication handler?

- ☐ Communication handler
- ☒ EDI Interface
- ☐ Application System
- ☐ EDI Translator

Explanation:

EDI Interface manipulates and routes data between the application system and the communication handler.

For your exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's computer system

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox services similar to post offices. The VAN receives all the outbound transactions from an organization, sort them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

EDI Interface -Interface function that manipulates and routes data between the application system and the communication handler. The interface consists of two components

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping. Data mapping is the process by which data are extracted from EDI translation process and integrated with the data or process of receiving company.

3. Application System - The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN).

Application System -The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

EDI Translator- The device translates data between standard format (ANSI X12) and trading partner's propriety information.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 178

Question 758

Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast address on multiple gateways in order to illicit responses from the computers behind the gateway where they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request packets?

- ☒ Reflected attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Explanation:

Reflected attack involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing replies to flood.

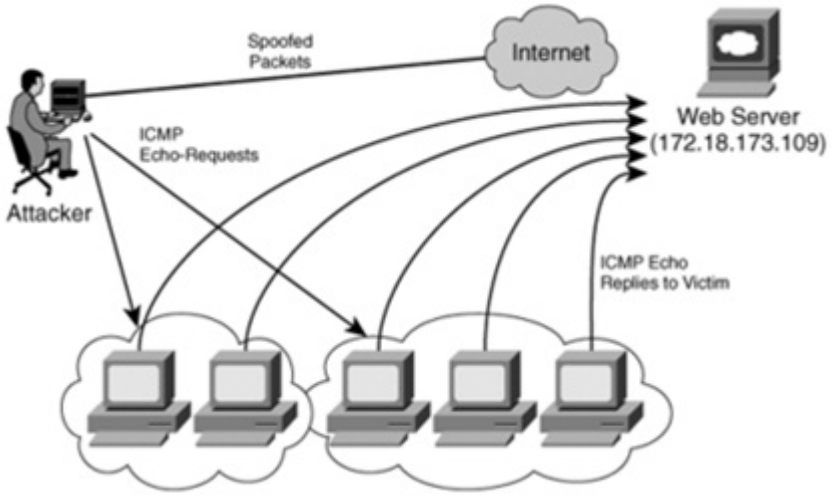
A distributed denial of service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. (This reflected attack form is sometimes called a "DRDOS".

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mix-configured networks, thereby enticing hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

Licensed to Berend Post berend.post@it-university.nl

In the surf attack, the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address. This means that each system on the victim's subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets—which is the victim's address. All of these response packets go to the victim system and overwhelm it because it is being bombarded with packets it does not necessarily know how to process. The victim system may freeze, crash, or reboot. The Smurf attack is illustrated in Figure below:

surf-attack



The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Licensed to Berend Post berend.post@it-university.nl

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 322

Question 759

An information security manager has identified and implemented migrating controls according to industry best practices. Which of the following is the GREATEST risk associated with this approach?

- ☐ Important security controls may be missed without senior management input.
- ☐ The cost of control implementation may be too high.
- ☐ The migration measures may not be updated in a timely manner.
- ☒ The security program may not be aligned with organizational objectives.

Question 760

Privileged account access is required to start an ad hoc batch job. Which of the following would MOST effectively detect unauthorized job execution?

- ☐ Requiring manual approval by an authorized user
- ☒ Executing the job through two-factor authentication
- ☐ Introducing job execution request procedures
- ☐ Reconciling user activity logs against authorizations

Question 761

Why does an IS auditor review an organization chart?

- ☐ To optimize the responsibilities and authority of individuals
- ☐ To control the responsibilities and authority of individuals
- ☒ To better understand the responsibilities and authority of individuals
- ☐ To identify project sponsors

Explanation:

Explanation:

The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

Licensed to Berend Post berend.post@it-university.nl

Question 762

During an audit of a reciprocal disaster recovery agreement between two companies, the IS auditor would be MOST concerned with the:

- ☐ allocation of resources during an emergency.
- ☒ maintenance of hardware and software compatibility.
- ☐ differences in IS policies and procedures.
- ☐ frequency of system testing.

Question 763

An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

- ☒ stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
- ☐ accept the project manager's position as the project manager is accountable for the outcome of the project.
- ☐ offer to work with the risk manager when one is appointed.
- ☐ inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Explanation:

Explanation: the majority of project risks can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with the risks. A project should have a clear link back to corporate strategy and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risks. Appointing a risk manager is a good practice but waiting until the project has been impacted by risks is misguided. Risk management needs to be forward looking; allowing risks to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risks have emerged or risk priorities have changed. The IS auditor has an obligation to the project sponsor and the organization to advise on appropriate project manage me practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

Licensed to Berend Post berend.post@it-university.nl

Question 764

After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

- ☐ Test and maintain the plan.
- ☐ Develop a specific plan.
- ☒ Develop recovery strategies.
- ☐ implement the plan.

Explanation:

Explanation:

The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested and implemented.

Question 765

Which of the following is the BEST indication of an effective incident management process?

- ☐ Percentage of incidents where root cause has been identified
- ☒ Percentage of incidents closed without escalation
- ☐ Number of calls to the help desk
- ☐ Number of incidents reviewed by the IT management

Question 766

The responsibility for authorizing access to application data should be with the:

- ☐ data custodian.
- ☐ database administrator (DBA).
- ☒ data owner.
- ☐ security administrator.

Explanation:

Explanation:

Data owners should have the authority and responsibility for granting access to the data and applications for which they are responsible. Data custodians are responsible only for storing and safeguarding the data. The database administrator (DBA) is responsible for managing the database and the security administrator is responsible for implementing and maintaining IS security. The ultimate responsibility for data resides with the data owner.

Licensed to Berend Post berend.post@it-university.nl

Question 767

A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

- ☐ Full-scale test with relocation of all departments, including IT, to the contingency site
- ☐ Walk-through test of a series of predefined scenarios with all critical personnel involved
- ☐ IT disaster recovery test with business departments involved in testing the critical applications
- ☒ Functional test of a scenario with limited IT involvement

Explanation:

Explanation:

After a tabletop exercise has been performed, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery. Since the IT part of the recovery has been tested for years, it would be more efficient to verify and optimize the business continuity plan (BCP) before actually involving IT in a full-scale test. The full-scale test would be the last step of the verification process before entering into a regular annual testing schedule. A full-scale test in the situation described might fail because it would be the first time that the plan is actually exercised, and a number of resources (including IT) and time would be wasted. The walk- through test is the most basic type of testing. Its intention is to make key staff familiar with the plan and discuss critical plan elements, rather than verifying its adequacy. The recovery of applications should always be verified and approved by the business instead of being purely IT-driven. A disaster recovery test would not help in verifying the administrative and organizational parts of the BCP which are not IT-related.

Question 768

The majority of software vulnerabilities result from a few known kinds of coding defects, such as (Choose five.):

- ☒ buffer overflows
- ☒ format string vulnerabilities
- ☒ integer overflow
- ☒ code injection
- ☒ command injection
- ☐ None of the choices.

Explanation:

Explanation:

The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common languages such as C and C++ are vulnerable to all of these

Licensed to Berend Post berend.post@it-university.nl

defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

Question 769

If the recovery time objective (RTO) increases:

- ☒ the disaster tolerance increases.
- ☐ the cost of recovery increases.
- ☐ a cold site cannot be used.
- ☐ the data backup frequency increases.

Explanation:

Explanation:

The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

Question 770

Which of the following is a feature of an intrusion detection system (IDS)?

- ☒ Gathering evidence on attack attempts
- ☐ Identifying weaknesses in the policy definition
- ☐ Blocking access to particular sites on the Internet
- ☐ Preventing certain users from accessing specific servers

Explanation:

Explanation:

An IDS can gather evidence on intrusive activity such as an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, while choice B requires a manual review, and therefore is outside the functionality of an IDS.

Question 771

During business process reengineering (BPR) of a bank's teller activities, an IS auditor should evaluate:

- ☒ the impact of changed business processes.
- ☐ the cost of new controls.
- ☐ BPR project plans.
- ☐ continuous improvement and monitoring plans.

Licensed to Berend Post berend.post@it-university.nl

Question 772

While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

- ☐ recommend the use of disk mirroring.
- ☐ review the adequacy of offsite storage.
- ☒ review the capacity management process.
- ☐ recommend the use of a compression algorithm.

Explanation:

Explanation:

Capacity management is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively. Business criticality must be considered before recommending a disk mirroring solution and offsite storage is unrelated to the problem.

Though data compression may save disk space, it could affect system performance.

Question 773

A security company and service provider have merged, and the CEO has requested one comprehensive set of security policies be developed for the newly formed company. The IS auditor's BEST recommendation would be to:

- ☒ conduct a policy gap assessment.
- ☐ adopt an industry standard security policy.
- ☐ implement the service provider's policies.
- ☐ implement the security company's policies.

Question 774

What is the BEST method to determine if IT resource spending is aligned with planned project spending?

- ☒ Earned value analysis (EVA)
- ☐ Gantt chart
- ☐ Return on investment (ROI) analysis
- ☐ Critical path analysis

Question 775

Which of the following is MOST likely to be included in a post-implementation review?

- ☒ Results of live processing
- ☐ Current sets of test data
- ☐ Test results
- ☐ Development methodology

Licensed to Berend Post berend.post@it-university.nl

Question 776

What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

- ☐ Paper
- ☒ Preparedness
- ☐ Walk-through
- ☐ Parallel

Explanation:

Explanation:

Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

Question 777

Which of the following is the BEST way to increase the effectiveness of security incident detection?

- ☐ Educating end users on identifying suspicious activity
- ☐ Establishing service level agreements (SLAs) with appropriate forensic service providers
- ☐ Determining containment activities based on the type of incident
- ☒ Documenting root cause analysis procedures

Question 778

Which of the following should be considered FIRST when implementing a risk management program?

- ☒ An understanding of the organization's threat, vulnerability and risk profile
- ☐ An understanding of the risk exposures and the potential consequences of compromise
- ☐ A determination of risk management priorities based on potential consequences
- ☐ A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Explanation:

Explanation:

Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

Licensed to Berend Post berend.post@it-university.nl

Question 779

A senior auditor is reviewing work papers prepared by a junior auditor indicating that a finding was removed after the auditee said they corrected the problem. Which of the following would be the MOST appropriate course of action for the senior auditor?

- ☐ Approve the work papers as written
- ☐ Refer the issue to the audit director
- ☒ Have the finding reinstated
- ☐ Ask the auditee to retest

Question 780

Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

- ☒ A system downtime log
- ☐ Vendors' reliability figures
- ☐ Regularly scheduled maintenance log
- ☐ A written preventive maintenance schedule

Explanation:

Explanation:

A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

Question 781

An IS auditor is reviewing the results of a business process improvement project. Which of the following should be performed FIRST?

- ☒ Evaluate control gaps between the old and the new processes.
- ☐ Develop compensating controls.
- ☐ Document the impact of control weaknesses in the process.
- ☐ Ensure that lessons learned during the change process are documented.

Question 782

A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

- ☒ Issues of privacy
- ☐ Wavelength can be absorbed by the human body
- ☐ RFID tags may not be removable
- ☐ RFID eliminates line-of-sight reading

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

Question 783

When responding to an ongoing denial of service (DoS) attack, an organization's FIRST course of action should be to:

- ☐ restore service
- ☒ minimize impact
- ☐ analyze the attack path
- ☐ investigate damage

Question 784

For a discretionary access control to be effective, it must:

- ☒ operate within the context of mandatory access controls.
- ☐ operate independently of mandatory access controls.
- ☐ enable users to override mandatory access controls when necessary.
- ☐ be specifically permitted by the security policy.

Explanation:

Explanation:

Mandatory access controls are prohibitive; anything that is not expressly permitted is forbidden. Only within this context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. When systems enforce mandatory access control policies, they must distinguish between these and the mandatory access policies that offer more flexibility.

Discretionary controls do not override access controls and they do not have to be permitted in the security policy to be effective.

Question 785

Which of the following would BEST assist senior management in evaluating IT performance as well as the alignment between corporate and IT strategic objectives?

- ☐ Enterprise architecture
- ☐ IT project value analysis
- ☒ Balanced scorecard
- ☐ Control self-assessment

Licensed to Berend Post berend.post@it-university.nl

Question 786

During an audit of a mission-critical system hosted in an outsourced data center, an IS auditor discovers that contracted routine maintenance for the alternate power generator was not performed. Which of the following should be the auditor's MAIN concern?

- ☐ Fraudulent behavior by the outsourcer charging for work not performed
- ☒ Failure of the alternate power generator during a power outage
- ☐ High repair costs if faulty generator parts are not detected in a timely manner
- ☐ Loss of warranty due to lack of system maintenance

Question 787

An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

- ☐ the setup is geographically dispersed.
- ☒ the network servers are clustered in a site.
- ☐ a hot site is ready for activation.
- ☐ diverse routing is implemented for the network.

Explanation:

Explanation:

A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backup if a site has been destroyed. A hot site would also be a good alternative for a single point-of-failure site.

Question 788

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

- ☐ comply with regulatory requirements.
- ☒ provide a basis for drawing reasonable conclusions.
- ☐ ensure complete audit coverage.
- ☐ perform the audit according to the defined scope.

Explanation:

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them.

Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

Licensed to Berend Post berend.post@it-university.nl

Question 789

Which of the following types of firewalls provide the GREATEST degree and granularity of control?

- ☐ Screaming router
- ☐ Packet filter
- ☒ Application gateway
- ☐ Circuit gateway

Explanation:

Explanation:

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and BJ work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4, and not from higher levels. A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

Question 790

An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

- ☒ exposure is greater, since information is available to unauthorized users.
- ☐ operating efficiency is enhanced, since anyone can print any report at any time.
- ☐ operating procedures are more effective, since information is easily available.
- ☐ user friendliness and flexibility is facilitated, since there is a smooth flow of information among users.

Explanation:

Explanation:

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

Licensed to Berend Post berend.post@it-university.nl

Question 791

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

- ☐ Define the recovery point objective (RPO).
- ☐ Analyze vulnerabilities.
- ☐ Confirm control effectiveness.
- ☒ Determine recovery priorities.

Question 792

As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following is necessary to restore these files?

- ☒ The previous day's backup file and the current transaction tape
- ☐ The previous day's transaction file and the current transaction tape
- ☐ The current transaction tape and the current hard copy transaction log
- ☐ The current hard copy transaction log and the previous day's transaction file

Explanation:

Explanation:

The previous day's backup file will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

Question 793

During an internal audit review of an HR recruitment system implementation, the IS auditor notes a number of defects were unresolved at the time the system went live. Which of the following is the auditor's MOST important task prior to formulating an audit opinion?

- ☐ Identify the root cause of the defects to confirm severity.
- ☒ Review the user acceptance test results.
- ☐ Verify risk acceptance by the project steering committee.
- ☐ Confirm the timeline for migration of the defects.

Licensed to Berend Post berend.post@it-university.nl

Question 794

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- ☒ Assimilation of the framework and intent of a written security policy by all appropriate parties
- ☐ Management support and approval for the implementation and maintenance of a security policy
- ☐ Enforcement of security rules by providing punitive actions for any violation of security rules
- ☐ Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Explanation:

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

Question 795

What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels?

- ☐ Business impact assessment
- ☐ Risk assessment
- ☒ IS assessment methods
- ☐ Key performance indicators (KPIs)

Explanation:

Explanation:

IS assessment methods allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

Licensed to Berend Post berend.post@it-university.nl

Question 796

Which of the following is of greatest concern to the IS auditor?

- ☒ Failure to report a successful attack on the network
- ☐ Failure to prevent a successful attack on the network
- ☐ Failure to recover from a successful attack on the network
- ☐ Failure to detect a successful attack on the network

Explanation:

Explanation:

Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

Question 797

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- ☐ Repeatable but Intuitive
- ☒ Defined
- ☐ Managed and Measurable
- ☐ Optimized

Explanation:

Explanation:

Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

Question 798

Which of the following testing procedure is used by an auditor to check whether a firm is following the rules and regulations applicable to an activity or practice?

- ☒ Compliance testing
- ☐ Sanity testing
- ☐ Recovery testing
- ☐ Substantive testing

Explanation:

Audit undertaken to confirm whether a firm is following the rules and regulations (prescribed by its internal authority or control system) applicable to an activity or practice.

Compliance testing is basically an audit of a system carried out against a known criterion. A compliance test may come in many different forms dependent on the request received but basically can be broken down into several different types:

Licensed to Berend Post berend.post@it-university.nl

Operating Systems and Applications: A verification that an operating system and/or applications are configured appropriately to the companies needs and lockdown requirements, thus providing adequate and robust controls to ensure that the Confidentiality, Integrity and Availability of the system will not be affected in its normal day to day operation.

Systems in development: A verification that the intended system under development meets the configuration and lockdown standards requested by the customer.

Management of IT and Enterprise Architecture: A verification that the in-place IT management infrastructure encompassing all aspects of system support has been put in place. This is to ensure effective change control, audit, business continuity and security procedures etc. have been formulated, documented and put in place.

Interconnection Policy: A verification that adequate security and business continuity controls governing the connection to other systems, be they Telecommunications, Intranets, Extranets and Internet etc. have been put in place, have been fully documented and correspond to the stated customer requirements.

The following answers are incorrect:

Substantive testing - A procedure used during accounting audits to check for errors in balance sheets and other financial documentation. A substantive test might involve checking a random sample of transactions for errors, comparing account balances to find discrepancies, or analysis and review of procedures used to execute and record transactions.

Sanity testing - Testing to determine if a new software version is performing well enough to accept it for a major testing effort. If application is crashing for initial use, then system is not stable enough for further testing and build or application is assigned to fix.

Recovery testing – Testing how well a system recovers from crashes, hardware failures, or other catastrophic problems.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 52 and 53

http://www.wikijob.co.uk/wiki/substantive-testing

Licensed to Berend Post berend.post@it-university.nl

Question 799

An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's FIRST course of action?

- ☐ Design mitigating controls for the exceptions.
- ☒ Prioritize the risk and implement treatment options.
- ☐ Inform respective risk owners of the impact of exceptions.
- ☐ Report the noncompliance to the board of directors.

Question 800

IT governance is PRIMARILY the responsibility of the:

- ☐ chief executive officer.
- ☒ board of directors.
- ☐ IT steering committee.
- ☐ audit committee.

Explanation:

Explanation:

IT governance is primarily the responsibility of the executives and shareholders {as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

Question 801

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

- ☐ audit trail of the versioning of the work papers.
- ☐ approval of the audit phases.
- ☐ access rights to the work papers.
- ☒ confidentiality of the work papers.

Explanation:

Explanation:

Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

Licensed to Berend Post berend.post@it-university.nl

Question 802

The MAIN benefit of using an integrated test facility (ITF) as an online auditing technique is that it enables:

- ☐ a cost-effective approach to application controls audit
- ☐ auditors to investigate fraudulent transactions
- ☒ auditors to test without impacting production data
- ☐ the integration of financial and audit tests

Question 803

To address an organization's disaster recovery requirements, backup intervals should not exceed the:

- ☐ service level objective (SLO).
- ☐ recovery time objective (RTO).
- ☒ recovery point objective (RPO).
- ☐ maximum acceptable outage (MAO).

Explanation:

Explanation:

The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster so as to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) so as to meet established targets. The resulting time for the service level agreement (SLA) will usually be longer than the RPO. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for RTO. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

Question 804

Which of the following is the MOST effective way to achieve the integration of information security governance into corporate governance?

- ☐ Ensure information security aligns with IT strategy.
- ☐ Provide periodic IT balanced scorecards to senior management.
- ☐ Align information security budget requests to organizational goals.
- ☒ Ensure information security efforts support business goals.

Licensed to Berend Post berend.post@it-university.nl

Question 805

Communicating which of the following would BEST encourage management to initiate appropriate actions following the receipt of report findings?

- ☐ Risk implications of the observations
- ☐ Strict deadlines to close all observations
- ☐ Statistical sampling used to derive observations
- ☒ Recommendations that align with the business strategy

Question 806

Effective IT governance requires organizational structures and processes to ensure that:

- ☐ the organization's strategies and objectives extend the IT strategy.
- ☐ the business strategy is derived from an IT strategy.
- ☐ IT governance is separate and distinct from the overall governance.
- ☒ the IT strategy extends the organization's strategies and objectives.

Explanation:

Explanation:

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

Question 807

Which of the following should be reviewed as part of a data integrity test?

- ☒ Completeness
- ☐ Confidentiality
- ☐ Data backup
- ☐ Redundancy

Question 808

A maturity model is useful in the assessment of IT service management because it:

- ☒ provides a benchmark for process improvement
- ☐ defines the level of control required to meet business needs
- ☐ indicates the service levels required for the business area
- ☐ specifies the mechanism needed to achieve defined service levels

Licensed to Berend Post berend.post@it-university.nl

Question 809

Which of the following should be of MOST influence to an information security manager when developing IT security policies?

- ☐ Past and current threats
- ☐ IT security framework
- ☐ Compliance with regulations
- ☒ Business strategy

Question 810

Which of the following layer of an enterprise data flow architecture represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☒ Data Mart layer
- ☐ Data access layer

Explanation:

Data Mart layer - Data mart represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Licensed to Berend Post berend.post@it-university.nl

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Licensed to Berend Post berend.post@it-university.nl

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Licensed to Berend Post berend.post@it-university.nl

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 811

Which of the following provides the MOST relevant information for proactively strengthening security settings?

- ☐ Bastion host
- ☐ Intrusion detection system
- ☒ Honeypot
- ☐ Intrusion prevention system

Explanation:

Explanation:

The design of a honeypot is such that it lures the hacker and provides clues as to the hacker's methods and strategies and the resources required to address such attacks. A bastion host does not provide information about an attack. Intrusion detection systems and intrusion prevention systems are designed to detect and address an attack in progress and stop it as soon as possible. A honeypot allows the attack to continue, so as to obtain information about the hacker's strategy and methods.

Question 812

During an ERP post-implementation review, it was noted that operating costs have been significantly higher than anticipated. Which of the following should the organization have done to detect this issue?

- ☐ Updated the project charter as major changes occurred
- ☐ Conducted periodic user satisfaction surveys
- ☐ Performed an analysis of system usage
- ☒ Monitored financial key performance indicators (KPIs)

Licensed to Berend Post berend.post@it-university.nl

Question 813

The MAIN purpose of documenting information security guidelines for use within a large, international organization is to:

- ☒ ensure that all business units have the same strategic security goals
- ☐ provide evidence for auditors that security practices are adequate
- ☐ explain the organization's preferred practices for security
- ☐ ensure that all business units implement identical security procedures

Question 814

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized modification?

- ☐ Availability
- ☐ Authenticity
- ☐ Confidentiality
- ☒ Integrity

Question 815

Disaster recovery planning (DRP) for a company's computer system usually focuses on:

- ☐ operations turnover procedures.
- ☐ strategic long-range planning.
- ☐ the probability that a disaster will occur.
- ☒ alternative procedures to process transactions.

Explanation:

Explanation:

It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

Question 816

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- ☒ there is an integration of IS and business staffs within projects.
- ☐ there is a clear definition of the IS mission and vision.
- ☐ a strategic information technology planning methodology is in place.
- ☐ the plan correlates business objectives to IS goals and objectives.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

Question 817

When conducting a requirements analysis for a project the BEST approach would be to:

- ☐ conduct a control self-assessment.
- ☒ consult key stakeholders.
- ☐ test operational deliverables.
- ☐ prototype the requirements.

Question 818

A virus typically consists of what major parts (Choose three.):

- ☒ a mechanism that allows them to infect other files and reproduce" a trigger that activates delivery of a "payload""
- ☒ a payload
- ☒ a signature
- ☐ None of the choices.

Explanation:

Explanation:

"A virus typically consist of three parts, which are a mechanism that allows them to infect other files and reproduce a trigger that activates delivery of a "payload" and the payload from which the virus often gets its name. The payload is what the virus does to the victim file."

Question 819

Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

- ☐ RPO
- ☒ RTO
- ☐ WRT
- ☐ MTD

Explanation:

Explanation:

The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Licensed to Berend Post berend.post@it-university.nl

It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. Decision time for users representative is not included.

The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

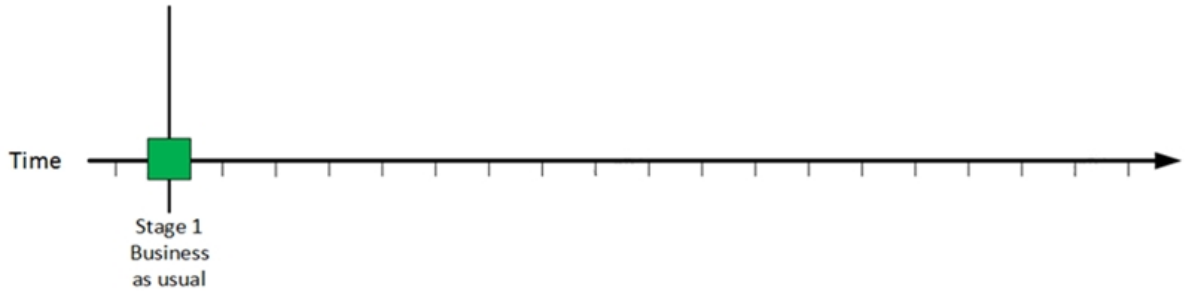
The RTO attaches to the business process and not the resources required to support the process.

The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs.

For your exam you should know below information about RPO, RTO, WRT and MTD :

Stage 1: Business as usual

Business as usual

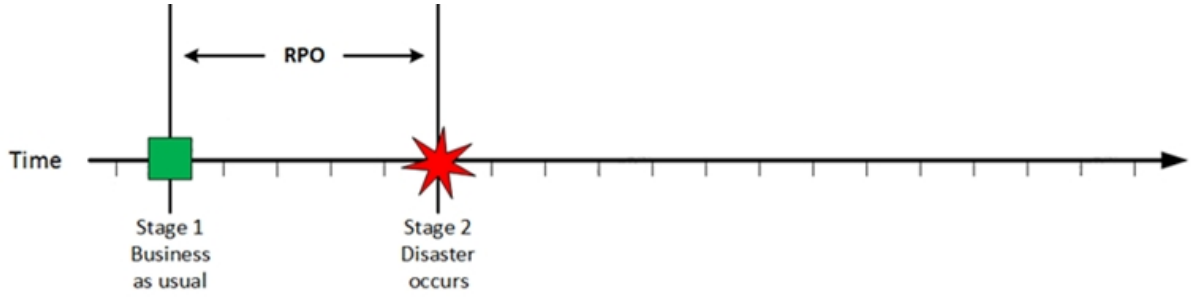


At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

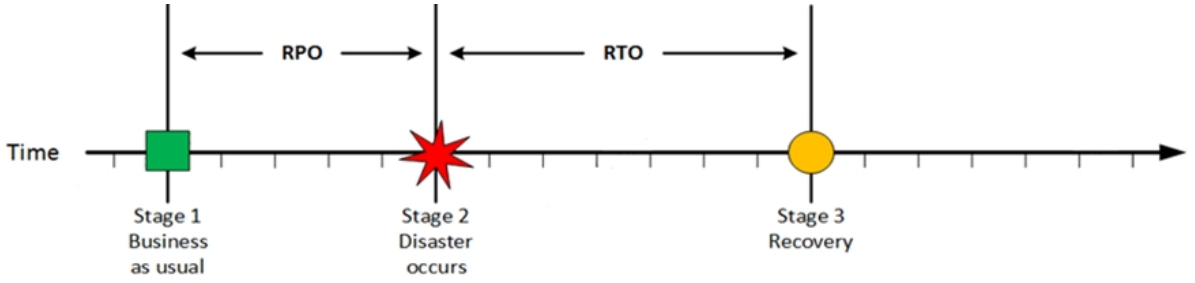
Licensed to Berend Post berend.post@it-university.nl



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

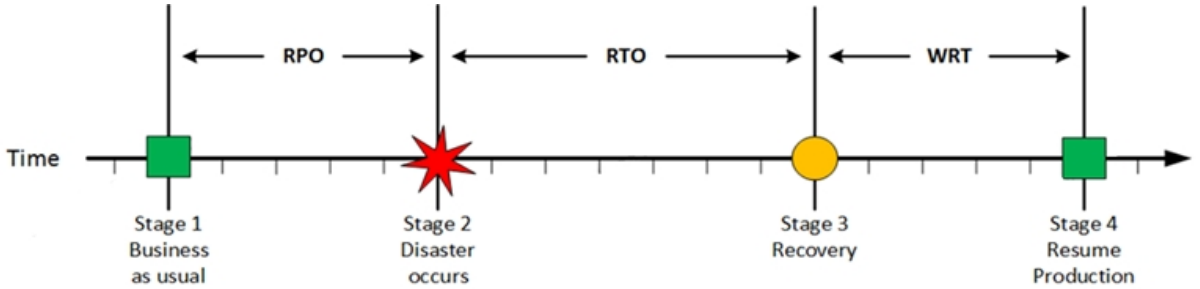
Recovery



At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

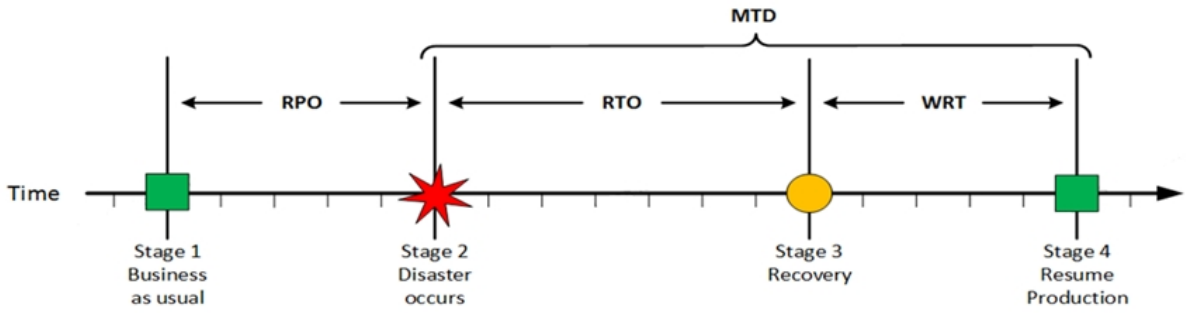
Resume Production



Licensed to Berend Post berend.post@it-university.nl

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Licensed to Berend Post berend.post@it-university.nl

References:

CISA review manual 2014 page number 284

http://en.wikipedia.org/wiki/Recovery_time_objective

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 820

To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

- ☐ Business recovery strategy
- ☐ Detailed plan development
- ☒ Business impact analysis (BIA)
- ☐ Testing and maintenance

Explanation:

Explanation:

End user involvement is critical in the BIA phase. During this phase the current operations of the business needs to be understood and the impact on the business of various disasters must be evaluated. End users are the appropriate persons to provide relevant information for these tasks, inadequate end user involvement in this stage could result in an inadequate understanding of business priorities and the plan not meeting the requirements of the organization.

Question 821

An auditor needs to be aware of technical controls which are used to protect computer from malware. Which of the following technical control interrupts DoS and ROM BIOS call and look for malware like action?

- ☐ Scanners
- ☒ Active Monitors
- ☐ Immunizer
- ☐ Behavior blocker

Explanation:

Active monitors interpret DoS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

For CISA exam you should know below mentioned different kinds of malware Controls

 Licensed to Berend Post berend.post@it-university.nl

A. Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present). Scanners examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other types of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Scanners -Look for sequences of bit called signature that are typical malware programs.

Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior.

Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 354 and 355

Question 822

An organization is within a jurisdiction where new regulations have recently been announced to restrict cross-border data transfer of personally identifiable information (PII). Which of the following IT decisions will MOST likely need to be assessed in the context of this change?

- ☐ Hosting the payroll system at an external cloud service provider
- ☐ Purchasing cyber insurance from an overseas insurance company
- ☐ Applying encryption to database hosting PII data
- ☒ Hiring IT consultants from overseas

Question 823

Which of the following is NOT a defined ISO basic task related to network management?

- ☐ Fault management
- ☐ Accounting resources
- ☐ Security management
- ☒ Communications management

Explanation:

Fault management: Detects the devices that present some kind of fault.

Licensed to Berend Post berend.post@it-university.nl

Configuration management: Allows users to know, define and change remotely the configuration of any device.

Accounting resources: Holds the records of the resource usage in the WAN.

Performance management: Monitors usage levels and sets alarms when a threshold has been surpassed.

Security management: Detects suspicious traffic or users and generates alarms accordingly.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

Question 824

Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

- ☒ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

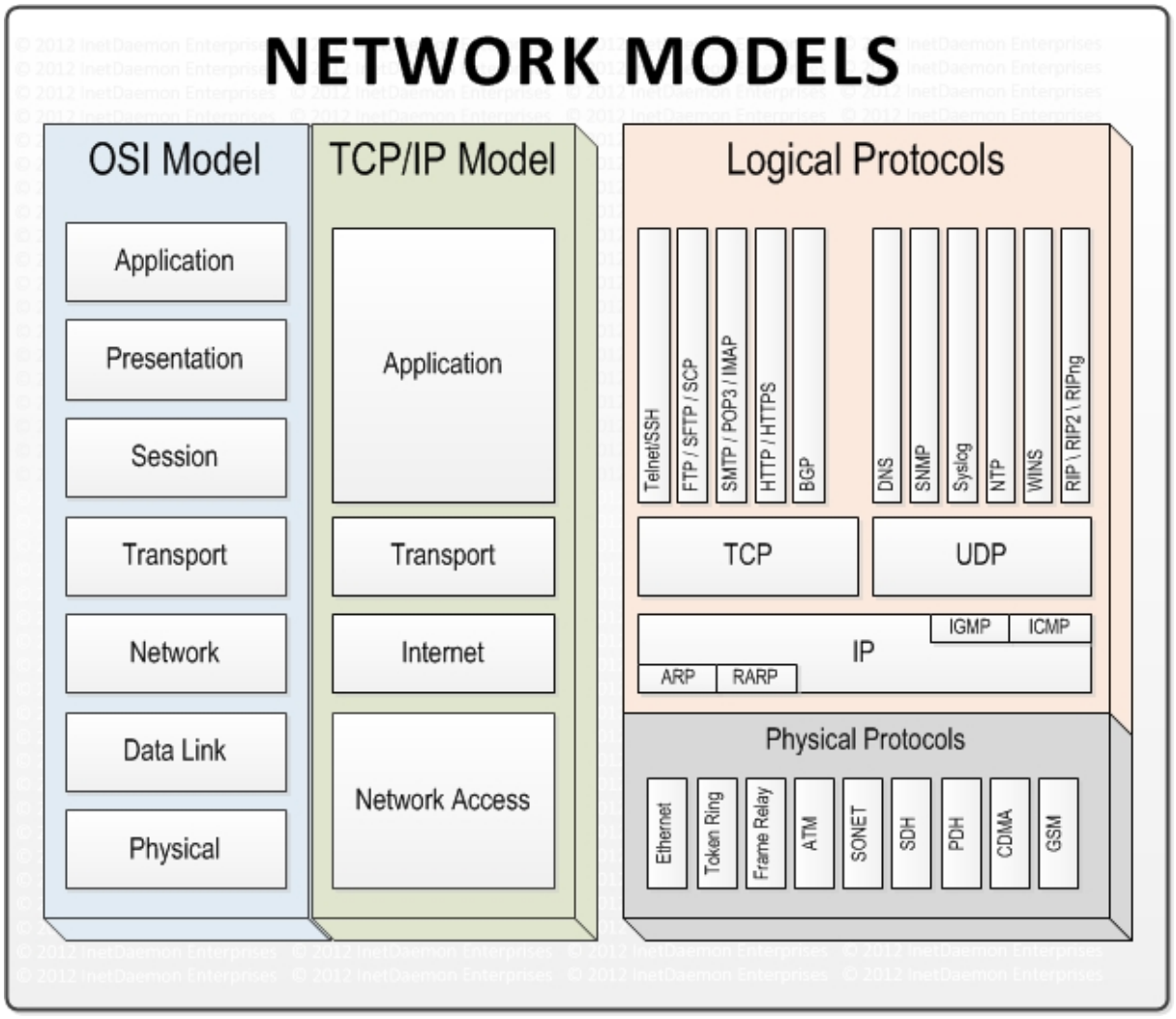
Explanation:

Application layer's PDU is data.

For your exam you should know below information about TCP/IP model:

Network models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

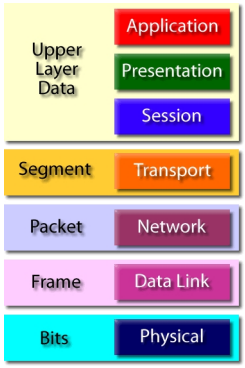
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

Segment – Transport layer PDU

Packet – Network interface layer PDU

Frame/bit – LAN or WAN interface layer PDU

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 825

When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

☐ The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
☐ Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
☒ A single implementation is planned, immediately decommissioning the legacy system.
☐ Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

Question 826

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- ☒ registration authority (RA).
- ☐ issuing certification authority (CA).
- ☐ subject CA.
- ☐ policy management authority.

Explanation:

Explanation:

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

Question 827

A stockbroker accepts orders over the Internet. Which of the following is the MOST appropriate control to ensure confidentiality of the orders?

- ☐ Virtual private network
- ☒ Public key encryption
- ☐ Data Encryption Standard (DES)
- ☐ Digital signature

Licensed to Berend Post berend.post@it-university.nl

Question 828

Which of the following is the MOST appropriate action to formalize IT governance in an organization?

- ☐ Evaluating the IT strategy
- ☐ Modifying IT goals and strategy
- ☒ Establishing an IT steering committee
- ☐ Implementing risk management

Question 829

Which of the following requirements in a document control standard would provide nonrepudiation to digitally signed legal documents?

- ☐ All digital signatures must include a hashing algorithm.
- ☒ All digitally signed documents must be stored in an encrypted database.
- ☐ All documents requiring digital signatures must be signed by both the customer and a witness.
- ☐ Only secure file transfer protocol (SFTP) may be used for digitally signed documentation.

Question 830

Integrating business continuity planning (BCP) into an IT project aids in:

- ☐ the retrofitting of the business continuity requirements.
- ☒ the development of a more comprehensive set of requirements.
- ☐ the development of a transaction flowchart.
- ☐ ensuring the application meets the user's needs.

Explanation:

Explanation:

Integrating business continuity planning (BCP) into the development process ensures complete coverage of the requirements through each phase of the project. Retrofitting of the business continuity plan's requirements occurs when BCP is not integrating into the development methodology. Transaction flowcharts aid in analyzing an application's controls. A business continuity plan will not directly address the detailed processing needs of the users.

Licensed to Berend Post berend.post@it-university.nl

Question 831

The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?

- ☐ Rewrite the patches and apply them
- ☐ Code review and application of available patches
- ☐ Develop in-house patches
- ☒ identify and test suitable patches before applying them

Explanation:

Explanation:

Suitable patches from the existing developers should be selected and tested before applying them. Rewriting the patches and applying them is not a correct answer because it would require skilled resources and time to rewrite the patches. Code review could be possible but tests need to be performed before applying the patches. Since the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.

Question 832

The PRIMARY objective of conducting a post-implementation review is to:

- ☐ determine if project management methodology was applied consistently
- ☒ verify that the information system meets the intended objectives
- ☐ determine if testing documentation was sufficient
- ☐ allow employees to provide feedback on the information system

Question 833

A sales representative is reviewing the organization's feedback blog and gets redirected to a site that sells illegal prescription drugs. The blog site is MOST likely susceptible to which of the following types of attacks?

- ☐ Directory harvesting
- ☐ SQL injection
- ☒ Cross-site scripting
- ☐ Phishing attack.

Licensed to Berend Post berend.post@it-university.nl

Question 834

Which of the following antispam filtering techniques would BEST prevent a valid, variable- length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

- ☐ Heuristic (rule-based)
- ☐ Signature-based
- ☐ Pattern matching
- ☒ Bayesian (statistical)

Explanation:

Explanation:

Bayesian filtering applies statistical modeling to messages, by performing a frequency analysis on each word within the message and then evaluating the message as a whole. Therefore, it can ignore a suspicious keyword if the entire message is within normal bounds. Heuristic filtering is less effective, since new exception rules may need to be defined when a valid message is labeled as spam. Signature-based filtering is useless against variable- length messages, because the calculated MD5 hash changes all the time. Finally, pattern matching is actually a degraded rule- based technique, where the rules operate at the word level using wildcards, and not at higher levels.

Question 835

The use of statistical sampling procedures helps minimize:

- ☒ Detection risk
- ☐ Business risk
- ☐ Controls risk
- ☐ Compliance risk

Explanation:

Explanation:

The use of statistical sampling procedures helps minimize detection risk.

Question 836

How does the process of systems auditing benefit from using a risk-based approach to audit planning?

- ☐ Controls testing starts earlier.
- ☒ Auditing resources are allocated to the areas of highest concern.
- ☐ Auditing risk is reduced.
- ☐ Controls testing is more thorough.

Explanation:

Explanation:

Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

Licensed to Berend Post berend.post@it-university.nl

Question 837

William has been assigned a changeover task. He has to break the older system into deliverable modules. Initially, the first module of the older system is phased out using the first module of a new system. Then, the second module of the old system is phased out, using the second module of the newer system and so forth until reaching the last module. Which of the following changeover system William needs to implement?

- ☐ Parallel changeover
- ☒ Phased changeover
- ☐ Abrupt changeover
- ☐ Pilot changeover

Explanation:

In phased changeover approach, the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.

Some of the risk areas that may exist in the phased changeover area includes:

Resource challenge

Extension of the project life cycle to cover two systems.

Change management for requirements and customizations to maintain ongoing support of the older systems.

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system.

Changeover to newer system involves four major steps or activities

Conversion of files and programs; test running on test bed

Installation of new hardware, operating system, application system and the migrated data.

Training employees or user in groups

Scheduling operations and test running for go-live or changeover

Some of the risk areas related to changeover includes:

Asset safeguarding

Licensed to Berend Post berend.post@it-university.nl

Data integrity

System effectiveness

Change management challenges

Duplicate or missing records

The following were incorrect answers:

Parallel changeover – This technique includes running the old system, then running both the old and new systems in parallel and finally full changing over to the new system after gaining confidence in the working of new system.

Abrupt changeover - In the abrupt changeover approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.

Pilot changeover – Not a valid changeover type.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 172

Question 838

When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

- ☐ Use the IP address of an existing file server or domain controller.
- ☒ Pause the scanning every few minutes to allow thresholds to reset.
- ☐ Conduct the scans during evening hours when no one is logged-in.
- ☐ Use multiple scanning tools since each tool has different characteristics.

Explanation:

Explanation:

Pausing the scanning every few minutes avoids overtaxing the network as well as exceeding thresholds that may trigger alert messages to the network administrator. Using the IP address of a server would result in an address contention that would attract attention. Conducting scans after hours would increase the chance of detection, since there would be less traffic to conceal ones activities. Using different tools could increase the likelihood that one of them would be detected by an intrusion detection system.

 Licensed to Berend Post berend.post@it-university.nl

Question 839

Which of the following is MOST critical for the effective implementation of IT governance?

- ☐ Internal auditor commitment
- ☒ Supportive corporate culture
- ☐ Strong risk management practices
- ☐ Documented policies

Question 840

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- ☐ Implementor
- ☒ Facilitator
- ☐ Developer
- ☐ Sponsor

Explanation:

Explanation:

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

Question 841

Which of the following is the BEST defense against a brute force attack?

- ☐ Discretionary access control
- ☐ Intruder detection lockout
- ☐ Mandatory access control
- ☒ Time-of-day restrictions

Question 842

An IS auditor evaluating logical access controls should FIRST:

- ☐ document the controls applied to the potential access paths to the system.
- ☐ test controls over the access paths to determine if they are functional.
- ☐ evaluate the security environment in relation to written policies and practices
- ☒ obtain an understanding of the security risks to information processing.

Explanation:

Explanation:

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the

Licensed to Berend Post berend.post@it-university.nl

adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

Question 843

Which of the following is MOST critical to the successful implementation of information security within an organization?

- ☐ Strong risk management skills exist within the information security group.
- ☐ Budget is allocated for information security tools.
- ☐ The information security manager is responsible for setting information security policy.
- ☒ Security is effectively marketed to all managers and employees.

Question 844

Which of the following software development methods is based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams?

- ☒ Agile Development
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

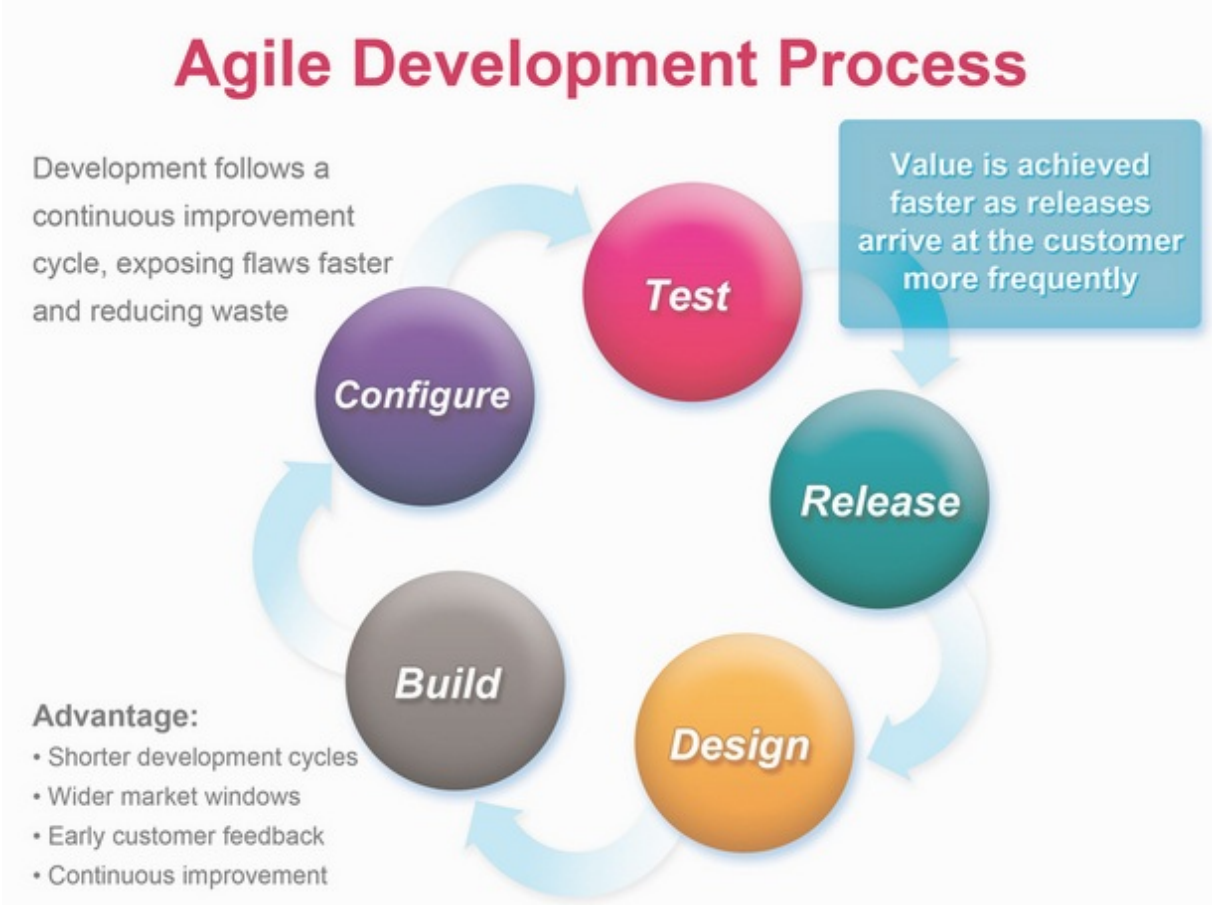
Explanation:

For your exam you should know below information about agile development:

Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to change. It is a conceptual framework that promotes foreseen tight iterations throughout the development cycle.

Agile Development

Licensed to Berend Post berend.post@it-university.nl



The Agile Manifesto introduced the term in 2001. Since then, the Agile Movement, with all its values, principles, methods, practices, tools, champions and practitioners, philosophies and cultures, has significantly changed the landscape of the modern software engineering and commercial software development in the Internet era.

Agile principles

The Agile Manifesto is based on twelve principles:

Customer satisfaction by rapid delivery of useful software

Welcome changing requirements, even late in development

Working software is delivered frequently (weeks rather than months)

Close, daily cooperation between business people and developers

Projects are built around motivated individuals, who should be trusted

Face-to-face conversation is the best form of communication (co-location)

Licensed to Berend Post berend.post@it-university.nl

Working software is the principal measure of progress

Sustainable development, able to maintain a constant pace

Continuous attention to technical excellence and good design

Simplicity—the art of maximizing the amount of work not done—is essential

Self-organizing teams

Regular adaptation to changing circumstances

What is Scrum?

Scrum is the most popular way of introducing Agility due to its simplicity and flexibility. Because of this popularity, many organizations claim to be “doing Scrum” but aren’t doing anything close to Scrum’s actual definition. Scrum emphasizes empirical feedback, team self-management, and striving to build properly tested product increments within short iterations. Doing Scrum as it’s actually defined usually comes into conflict with existing habits at established non-Agile organizations.

The following were incorrect answers:

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.

Component Based Development - It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 194

Licensed to Berend Post berend.post@it-university.nl

Question 845

Off-site data storage should be kept synchronized when preparing for recovery of time- sensitive data such as that resulting from which of the following?

- ☐ Financial reporting
- ☐ Sales reporting
- ☐ Inventory reporting
- ☒ Transaction processing

Explanation:

Explanation:

Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.

Question 846

A bank is relocating its servers to a vendor that provides data center hosting services to multiple clients. Which of the following controls would restrict other clients from physical access to the bank's servers?

- ☐ Closed-circuit television cameras
- ☒ Locking server cages
- ☐ Biometric access at all data center entrances
- ☐ 24-hour security guards

Question 847

Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

- ☒ DNS
- ☐ FTP
- ☐ SSH
- ☐ SMTP

Explanation:

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

For your exam you should know below information general Internet terminology:

Licensed to Berend Post berend.post@it-university.nl

Network access point -Internet service providers access internet using net access point. A Network Access Point (NAP) was a public network exchange facility where Internet service providers (ISPs) connected with one another in peering arrangements. The NAPs were a key component in the transition from the 1990s NSFNET era (when many networks were government sponsored and commercial traffic was prohibited) to the commercial Internet providers of today. They were often points of considerable Internet congestion.

Internet Service Provider (ISP) - An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, co-location.

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates

 Licensed to Berend Post berend.post@it-university.nl

and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

The following answers are incorrect:

SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 273 and 274

Licensed to Berend Post berend.post@it-university.nl

Question 848

A digital signature contains a message digest to:

- ☒ show if the message has been altered after transmission.
- ☐ define the encryption algorithm.
- ☐ confirm the identity of the originator.
- ☐ enable message transmission in a digital format.

Explanation:

Explanation:

The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. It does not define the algorithm or enable the transmission in digital format and has no effect on the identity of the user; it is there to ensure integrity rather than identity.

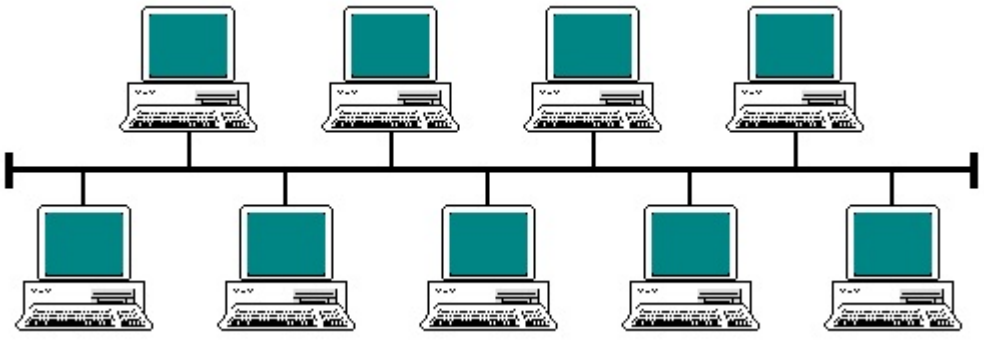
Question 849

An organization has outsourced its data leakage monitoring to an Internet service provider (ISP). Which of the following is the BEST way for an IS auditor to determine the effectiveness of this service?

- ☐ Verify the ISP has staff to deal with data leakage
- ☐ Review the ISP's external audit report
- ☒ Review the data leakage clause in the SLA
- ☐ Simulate a data leakage incident

Question 850

Identify the LAN topology from below diagram presented below:



bus topology

- ☒ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Explanation:

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know the information below related to LAN topologies:

LAN Topologies

Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

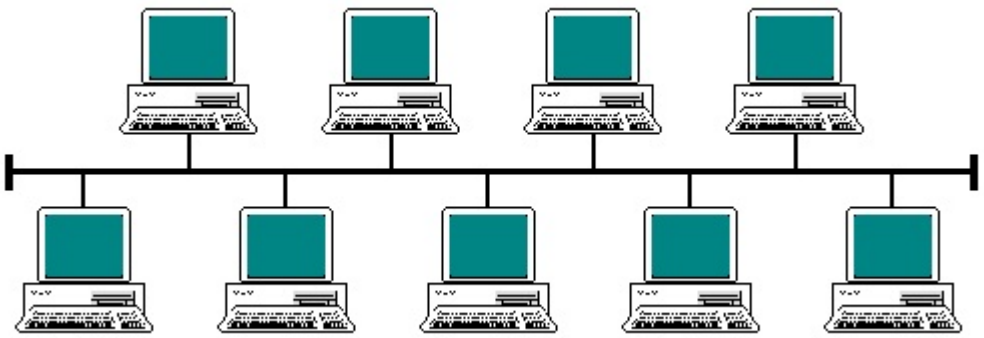
Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology



Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly

Licensed to Berend Post berend.post@it-university.nl

referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

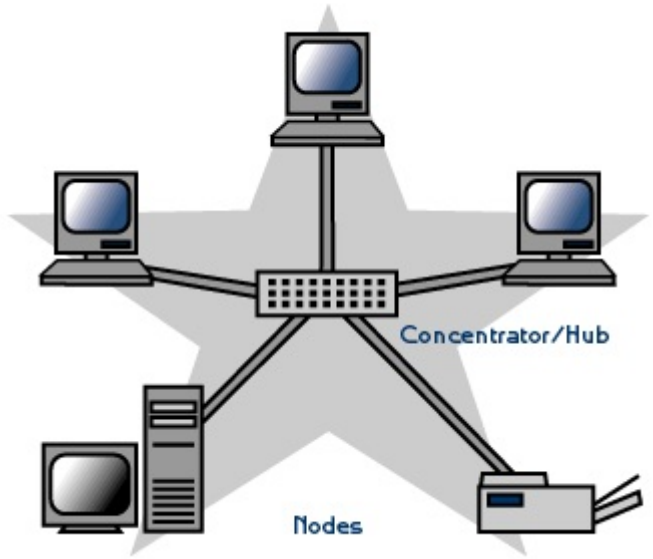
The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure.

Star Topology

Licensed to Berend Post berend.post@it-university.nl

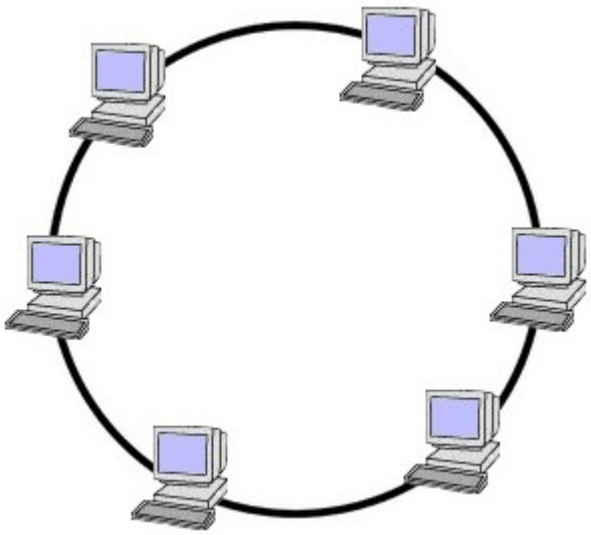


Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology



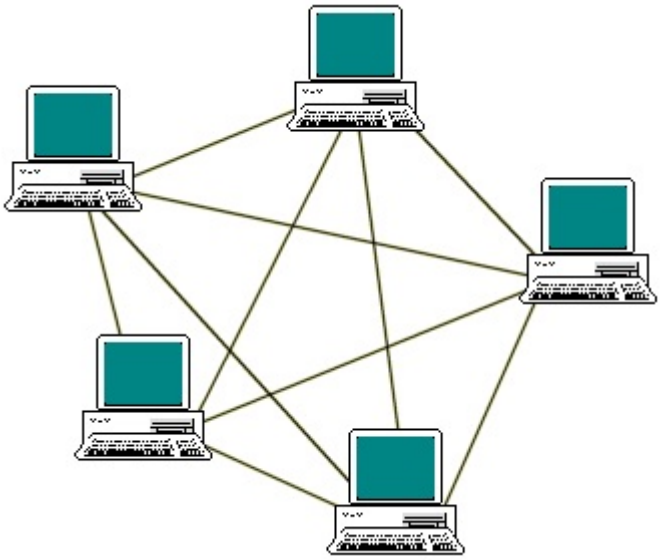
Licensed to Berend Post berend.post@it-university.nl

Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.

Mesh Topology



Fully connected mesh topology

A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

The other options presented are not valid.

The following reference(s) were/was used to create this question:

CISA review manual 2014, Page number 262

Question 851

An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

- ☐ Piggybacking
- ☐ Dumpster diving
- ☒ Shoulder surfing
- ☐ Impersonation

Explanation:

Explanation:

If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' then it would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

Question 852

Which of the following is MOST relevant for an information security manager to communicate to IT operations?

- ☐ The level of inherent risk
- ☐ Vulnerability assessments
- ☐ Threat assessments
- ☒ The level of exposure

Licensed to Berend Post berend.post@it-university.nl

Question 853

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

- ☒ increases in quality can be achieved, even if resource allocation is decreased.
- ☐ increases in quality are only achieved if resource allocation is increased.
- ☐ decreases in delivery time can be achieved, even if resource allocation is decreased.
- ☐ decreases in delivery time can only be achieved if quality is decreased.

Explanation:

Explanation:

The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

Question 854

Which of the following is MOST important in determining a project's feasibility?

- ☐ The organization's main competitor has initiated a similar project.
- ☐ The IT steering committee endorses the project.
- ☐ A project management methodology is established.
- ☒ The project's value is established in an approved business case.

Question 855

In attribute sampling, what is the relationship between expected error rate and sample size?

- ☒ The expected error rate does not affect the sample size
- ☐ The greater the expected error rate, the smaller the sample size
- ☐ The greater the expected error rate, the grater the sample size
- ☐ The greater the sample size, the lower the expected error rate

Question 856

An intruder accesses an application server and makes changes to the system log. Which of the following would enable the identification of the changes?

- ☐ Mirroring the system log on another server
- ☒ Simultaneously duplicating the system log on a write-once disk
- ☐ Write-protecting the directory containing the system log
- ☐ Storing the backup of the system log offsite

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

Question 857

Which of the following cryptography demands less computational power and offers more security per bit?

- ☐ Quantum cryptography
- ☒ Elliptic Curve Cryptography (ECC)
- ☐ Symmetric Key Cryptography
- ☐ Asymmetric Key Cryptography

Explanation:

ECC demands less computational power and, therefore offers more security per bit. For example, an ECC with a 160-bit key offer the same security as an RSA based system with a 1024-bit key.

ECC is a variant and more efficient form of a public key cryptography (how tom manage more security out of minimum resources) gaining prominence is the ECC. ECC works well on a network computer requires strong cryptography but have some limitation such as bandwidth and processing power. This is even more important with devices such as smart cards, wireless phones and other mobile devices.

The following were incorrect answers:

Quantum Cryptography - Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection. Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

Symmetric Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

 Licensed to Berend Post berend.post@it-university.nl

Asymmetric Encryption - The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is asymmetric encryption, in which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 349 and 350

http://support.microsoft.com/kb/246071

Question 858

Which of the following is MOST important for an IS auditor to consider during a review of the IT governance of an organization?

- ☐ Funding allocations
- ☐ Risk management methodology
- ☒ Defined service levels
- ☐ Decision making responsibilities

Question 859

Which of the following would be an auditor's GREATEST concern when reviewing data inputs from spreadsheets into the core finance system?

- ☒ Undocumented code formats data and transmits directly to the database.
- ☐ There is not a complete inventory of spreadsheets, and file naming is inconsistent.
- ☐ Spreadsheets are accessible by all members of the finance department.
- ☐ The department data protection policy has not been reviewed or updated for two years.

Licensed to Berend Post berend.post@it-university.nl

Question 860

Which of the following attacks targets the Secure Sockets Layer (SSL)?

- ☒ Man-in-the middle
- ☐ Dictionary
- ☐ Password sniffing
- ☐ Phishing

Explanation:

Explanation:

Attackers can establish a fake Secure Sockets Layer (SSL) server to accept user's SSL traffic and then route to the real SSL server, so that sensitive information can be discovered. A dictionary attack that has been launched to discover passwords would not attack SSL since SSL does not rely on passwords. SSL traffic is encrypted; thus it is not possible to sniff the password. A phishing attack targets a user and not SSL Phishing attacks attempt to have the user surrender private information by falsely claiming to be a trusted person or enterprise.

Question 861

Regarding a disaster recovery plan, the role of an IS auditor should include:

- ☐ identifying critical applications.
- ☐ determining the external service providers involved in a recovery test.
- ☒ observing the tests of the disaster recovery plan. determining the criteria for
- ☐ establishing a recovery time objective (RTO).

Explanation:

Explanation:

The IS auditor should be present when disaster recovery plans are tested, to ensure that the test meets the targets for restoration, and the recovery procedures are effective and efficient. As appropriate, the auditor should provide a report of the test results. All other choices are a responsibility of management.

Question 862

An IS auditor has assessed a payroll service provider's security policy and finds significant topics are missing. Which of the following is the auditor's BEST course of action?

- ☐ Recommend the service provider update their policy.
- ☐ Notify the service provider of the discrepancies.
- ☒ Report the risk to internal management.
- ☐ Recommend replacement of the service provider.

Licensed to Berend Post berend.post@it-university.nl

Question 863

TEMPEST is a hardware for which of the following purposes?

- ☒ Eavedropping
- ☐ Social engineering
- ☐ Virus scanning
- ☐ Firewalling
- ☐ None of the choices.

Explanation:

Explanation:

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

Question 864

Which of the following should be of MOST concern to an IS auditor reviewing the public key infrastructure (PKI) for enterprise e-mail?

- ☐ The private key certificate has not been updated.
- ☒ The certificate revocation list has not been updated.
- ☐ The certificate practice statement has not been published.
- ☐ The PKI policy has not been updated within the last year.

Question 865

Which of the following is BEST suited for secure communications within a small group?

- ☐ Key distribution center
- ☐ Certification authority
- ☒ Web of trust
- ☐ Kerberos Authentication System

Explanation:

Explanation:

Web of trust is a key distribution method suitable for communication in a small group. It ensures pretty good privacy (PGP) and distributes the public keys of users within a group. Key distribution center is a distribution method suitable for internal communication for a large group within an institution, and it will distribute symmetric keys for each session. Certification authority is a trusted third party that ensures the authenticity of the owner of the certificate. This is necessary for large groups and formal communication. A Kerberos Authentication System extends the function of a key distribution center, by generating 'tickets' to define the facilities on networked machines which are accessible to each user.

Licensed to Berend Post berend.post@it-university.nl

Question 866

A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

- ☐ compute the amortization of the related assets.
- ☐ calculate a return on investment (ROI).
- ☒ apply a qualitative approach.
- ☐ spend the time needed to define exactly the loss amount.

Explanation:

Explanation:

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor {e.g., one is a very low impact to the business and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, ant at the end of the day, the result will be a not well-supported evaluation.

Question 867

An IS auditor has been asked to assess the security of a recently migrated database system that contains personal and financial data for a bank's customers. Which of the following controls is MOST important for the auditor to confirm it in place?

- ☐ The default configurations have been changed.
- ☒ All tables in the database are normalized.
- ☐ The service port used by the database server has been changed.
- ☐ The default administration account is used after changing the account password.

Question 868

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

- ☐ an incident involving unauthorized access to data cannot be tied to a specific user.
- ☐ when multiple sessions with the same application ID collide, the database locks up.
- ☒ users can gain direct access to the application ID and circumvent data controls.
- ☐ the database becomes unavailable if the password of the application ID expires.

Licensed to Berend Post berend.post@it-university.nl

Question 869

Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

- ☐ RPO
- ☐ RTO
- ☒ WRT
- ☐ MTD

Explanation:

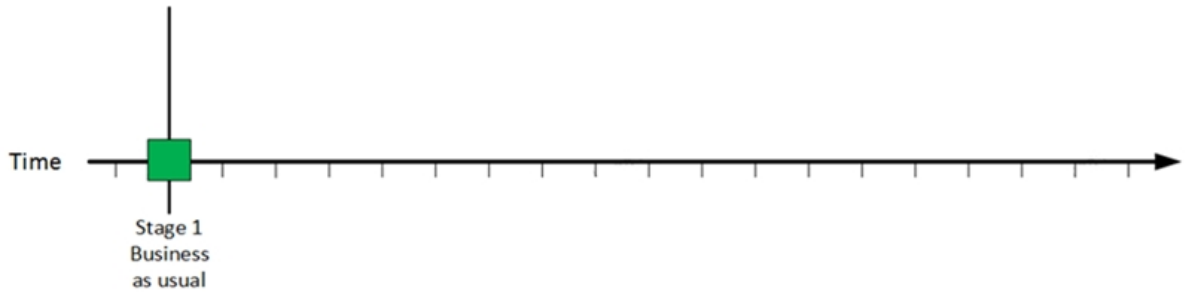
Explanation:

The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

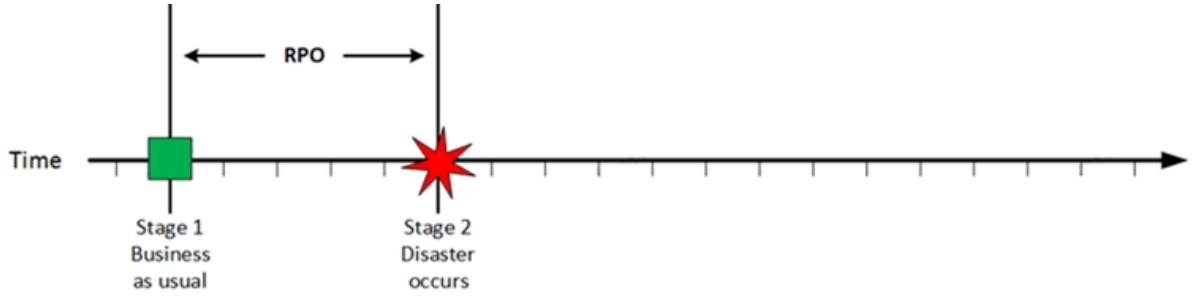


At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

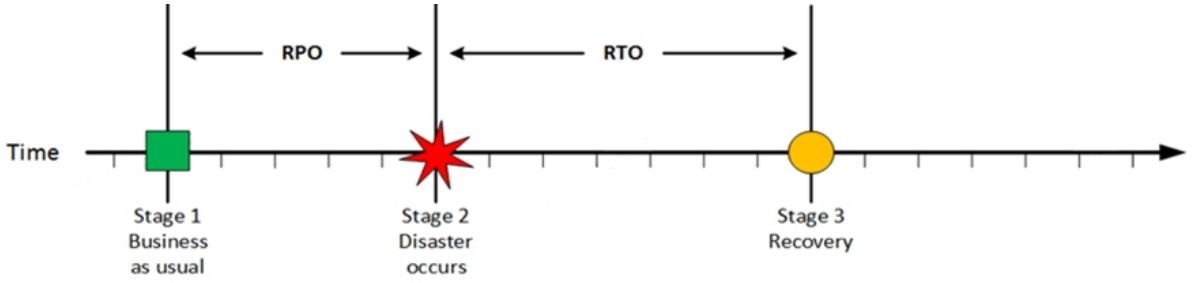
Licensed to Berend Post berend.post@it-university.nl



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

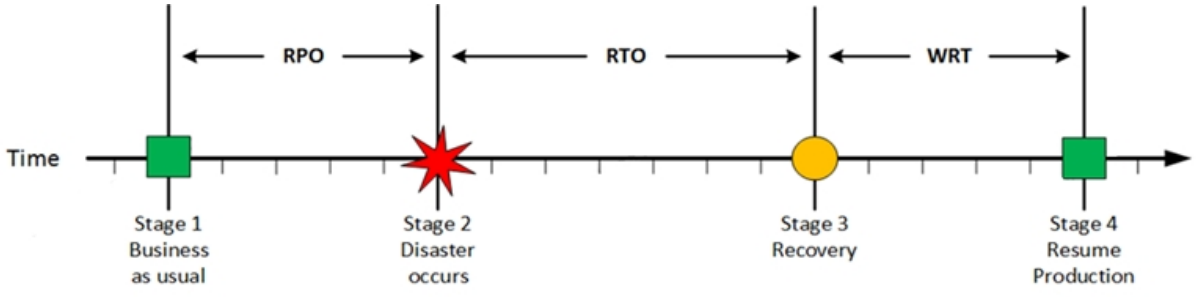
Recovery



At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

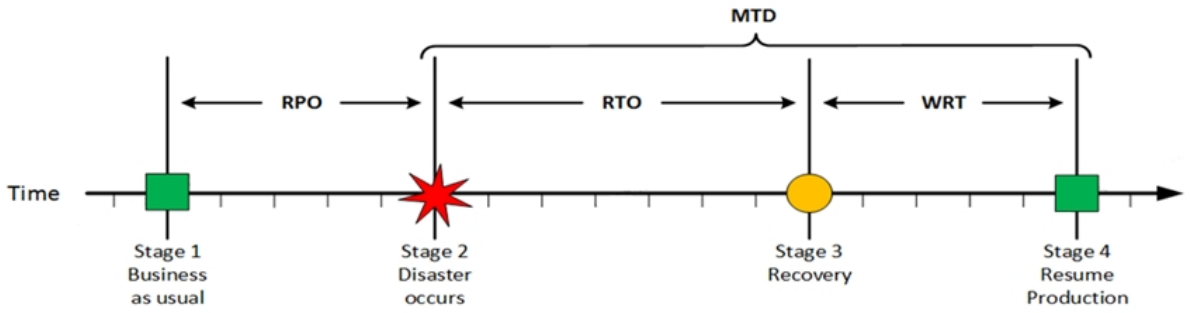
Resume Production



Licensed to Berend Post berend.post@it-university.nl

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Licensed to Berend Post berend.post@it-university.nl

References:

CISA review manual 2014 page number 284

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 870

An IS audit reveals that an organization is not proactively addressing known vulnerabilities. Which of the following should the IS auditor recommend the organization do FIRST?

- ☐ Verify the disaster recovery plan (DRP) has been tested.
- ☐ Ensure the intrusion prevention system (IPS) is effective.
- ☐ Confirm the incident response team understands the issue.
- ☒ Assess the security risks to the business.

Question 871

Which of the following is a substantive test?

- ☐ Checking a list of exception reports
- ☐ Ensuring approval for parameter changes
- ☒ Using a statistical sample to inventory the tape library
- ☐ Reviewing password history reports

Explanation:

Explanation:

A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

Question 872

The BEST way to evaluate a shared control environment is to obtain an assurance report and review which of the following?

- ☐ Control self-assessment (CSA)
- ☐ Service level agreement (SLA)
- ☒ Master service agreement
- ☐ Complementary user entity controls

Licensed to Berend Post berend.post@it-university.nl

Question 873

Which of the following is the MOST important objective of data protection?

- ☐ identifying persons who need access to information
- ☒ Ensuring the integrity of information
- ☐ Denying or authorizing access to the IS system
- ☐ Monitoring logical accesses

Explanation:

Explanation:

Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

Question 874

Which of the following is a benefit of using callback devices?

- ☒ Provide an audit trail
- ☐ Can be used in a switchboard environment
- ☐ Permit unlimited user mobility
- ☐ Allow call forwarding

Explanation:

Explanation:

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

Question 875

An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would BEST mitigate the risk of undetected and unauthorized program changes to the production environment?

- ☐ Commands typed on the command line are logged
- ☒ Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs
- ☐ Access to the operating system command line is granted through an access restriction tool with preapproved rights
- ☐ Software development tools and compilers have been removed from the production environment

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The matching of hash keys over time would allow detection of changes to files. Choice A is incorrect because having a log is not a control, reviewing the log is a control. Choice C is incorrect because the access was already granted-it does not matter how. Choice D is wrong because files can be copied to and from the production environment.

Question 876

The risk of communication failure in an e-commerce environment is BEST minimized through the use of:

- ☒ alternative or diverse routing
- ☐ compression software to minimize transmission duration
- ☐ a packet filtering firewall to reroute messages
- ☐ functional or message acknowledgments

Question 877

Which of the following will prevent dangling tuples in a database?

- ☐ Cyclic integrity
- ☐ Domain integrity
- ☐ Relational integrity
- ☒ Referential integrity

Explanation:

Explanation:

Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

Question 878

Which of the following is MOST important to include in a business continuity plan (BCP)?

- ☐ Vendor contact information
- ☒ Documentation of critical systems
- ☐ Documentation of data center floor plans
- ☐ Backup site location information

Licensed to Berend Post berend.post@it-university.nl

Question 879

During which of the following phases in system development would user acceptance test plans normally be prepared?

- ☐ Feasibility study
- ☒ Requirements definition
- ☐ implementation planning
- ☐ Postimplementation review

Explanation:

Explanation:

During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document hot the system functionality can be tested ensure it meets their stated needs. The feasibility study is too early for such detailed user involvement, and the implementation planning and postimplementation review phases are too late. An IS auditor should know at what point user testing should be planned to ensure it is most effective and efficient.

Question 880

As an IS auditor it is very important to understand the importance of job scheduling. Which of the following statement is NOT true about job scheduler or job scheduling software?

- ☒ Job information is set up only once, which increase the probability of an error.
- ☐ Records are maintained of all job success and failures.
- ☐ Reliance on operator is reduced.
- ☐ Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

Explanation:

The NOT keyword is used in this question. You need to find out an option which is not true about job scheduling.

Below are some advantages of job scheduling or using job scheduling software.

Job information is set up only once, reduce the probability of an error.

Records are maintained of all job success and failures.

Reliance on operator is reduced.

Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

For your exam you should know the information below:

Licensed to Berend Post berend.post@it-university.nl

A job scheduler is a computer application for controlling unattended background program execution (commonly called batch processing).

Synonyms are batch system, Distributed Resource Management System (DRMS), and Distributed Resource Manager (DRM). Today's job schedulers, often termed workload automation, typically provide a graphical user interface and a single point of control for definition and monitoring of background executions in a distributed network of computers. Increasingly, job schedulers are required to orchestrate the integration of real-time business activities with traditional background IT processing across different operating system platforms and business application environments.

Job scheduling should not be confused with process scheduling, which is the assignment of currently running processes to CPUs by the operating system.

Basic features expected of job scheduler software include:

interfaces which help to define workflows and/or job dependencies

automatic submission of executions

interfaces to monitor the executions

priorities and/or queues to control the execution order of unrelated jobs

If software from a completely different area includes all or some of those features, this software is consider to have job scheduling capabilities.

Most operating systems (such as Unix and Windows) provide basic job scheduling capabilities, for example: croon. Web hosting services provide job scheduling capabilities through a control panel or a webcron solution. Many programs such as DBMS, backup, ERPs, and BPM also include relevant job-scheduling capabilities. Operating system ("OS") or point program supplied job-scheduling will not usually provide the ability to schedule beyond a single OS instance or outside the remit of the specific program. Organizations needing to automate unrelated IT workload may also leverage further advanced features from a job scheduler, such as:

real-time scheduling based on external, unpredictable events

automatic restart and recovery in event of failures

alerting and notification to operations personnel

generation of incident reports

audit trails for regulatory compliance purposes

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

The other options are correctly defined about job scheduling

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 242

http://en.wikipedia.org/wiki/Job_scheduler

Question 881

The FIRST step in establishing a firewall security policy is to determine the:

- ☐ necessary logical access rights.
- ☐ expected data throughput.
- ☒ business requirements.
- ☐ existing firewall configuration.

Question 882

Which of the following is the MOST important factor to consider when establishing a severity hierarchy for information security incidents?

- ☐ Management support
- ☒ Business impact
- ☐ Regulatory compliance
- ☐ Residual risk

Question 883

Which of the following is the PRIMARY advantage of single sign-on (SSO)?

- ☐ Improves system performance
- ☐ Ensures good password practices
- ☐ Improves security
- ☒ Reduces administrative workload.

Licensed to Berend Post berend.post@it-university.nl

Question 884

A critical function of a firewall is to act as a:

- ☐ special router that connects the Internet to a LAN.
- ☒ device for preventing authorized users from accessing the LAN.
- ☐ server used to connect authorized users to private trusted network resources.
- ☐ proxy server to increase the speed of access to authorized users.

Explanation:

Explanation:

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

Question 885

If a database is restored using before-image dumps, where should the process begin following an interruption?

- ☒ Before the last transaction
- ☐ After the last transaction
- ☐ As the first transaction after the latest checkpoint
- ☐ At the last transaction before the latest checkpoint

Explanation:

Explanation:

If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

Question 886

Which of the following would be the MOST secure firewall system?

- ☐ Screened-host firewall
- ☒ Screened-subnet firewall
- ☐ Dual-homed firewall
- ☐ Stateful-inspection firewall

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A screened-subnet firewall, also used as a demilitarized zone (DMZ), utilizes two packet filtering routers and a bastion host. This provides the most secure firewall system, since it supports both network- and application-level security while defining a separate DMZ network. A screened-host firewall utilizes a packet filtering router and a bastion host. This approach implements basic network layer security (packet filtering) and application server security (proxy services). A dual- homed firewall system is a more restrictive form of a screened-host firewall system, configuring one interface for information servers and another for private network host computers. A stateful-inspection firewall working at the transport layer keeps track of the destination IP address of each packet that leaves the organization's internal network and allows a reply from the recorded IP addresses.

Question 887

Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

- ☒ Accuracy of the source data
- ☐ Credibility of the data source
- ☐ Accuracy of the extraction process
- ☐ Accuracy of the data transformation

Explanation:

Explanation:

Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source, accurate extraction processes and accurate transformation routines are all important, but would not change inaccurate data into quality (accurate) data.

Question 888

When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

- ☐ Number of nonthreatening events identified as threatening
- ☒ Attacks not being identified by the system
- ☐ Reports/logs being produced by an automated tool
- ☐ Legitimate traffic being blocked by the system

Explanation:

Explanation:

Attacks not being identified by the system present a higher risk, because they are unknown and no action will be taken to address the attack. Although the number of false-positives is a serious issue, the problem will be known and can be corrected. Often, IDS reports are first analyzed by an automated tool to eliminate known false-positives, which generally are not a problem. An IDS does not block any traffic.

Licensed to Berend Post berend.post@it-university.nl

Question 889

A local area network (LAN) administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager
- ☒ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Explanation:

Explanation:

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

Question 890

Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?

- ☒ Pretexting
- ☐ Backgrounding
- ☐ Check making
- ☐ Bounce checking
- ☐ None of the choices.

Explanation:

Explanation:

Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action and is usually done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information.

Question 891

Which of the following is a method to prevent disclosure of classified documents printed on a shared printer?

- ☐ Requiring a key code to be entered on the printer to produce hardcopy
- ☐ Producing a header page with classification level for printed documents
- ☐ Encrypting the data stream between the user's computer and the printer
- ☒ Using passwords to allow authorized users to send documents to the printer

Licensed to Berend Post berend.post@it-university.nl

Question 892

An IS auditor is a member of an application development team that is selecting software. Which of the following would impair the auditor's independence?

- ☐ Verifying the weighting of each selection criteria
- ☒ Approving the vendor selection methodology
- ☐ Reviewing the request for proposal (RFP)
- ☐ Witnessing the vendor selection process

Question 893

Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called a:

- ☐ feedback error control.
- ☐ block sum check.
- ☒ forward error control.
- ☐ cyclic redundancy check.

Explanation:

Explanation:

Forward error control involves transmitting additional redundant information with each character or frame to facilitate detection and correction of errors, in feedback error control, only enough additional information is transmitted so the receiver can identify that an error has occurred.

Choices B and D are both error detection methods but not error correction methods. Block sum check is an extension of parity check wherein an additional set of parity bits is computed for a block of characters. A cyclic redundancy check is a technique wherein a single set of check digits is generated, based on the contents of the frame, for each frame transmitted.

Question 894

Which of the following type of network service stores information about the various resources in a central database on a network and help network devices locate services?

- ☐ DHCP
- ☐ DNS
- ☒ Directory Service
- ☐ Network Management

Explanation:

A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.

Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:

Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.

Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.

Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Question 895

An organization has installed blade server technology in its data center. To determine whether higher cooling demands are maintained, which of the following should the IS auditor review?

- ☐ Ventilation systems
- ☐ Uninterruptible power supply (UPS) systems
- ☒ Air conditioning capacity
- ☐ Duct maintenance

Question 896

In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

- ☐ connectionless integrity.
- ☐ data origin authentication.
- ☐ antireplay service.
- ☒ confidentiality.

Explanation:

Explanation:

Both protocols support choices A, B and C, but only the ESP protocol provides confidentiality via encryption.

Licensed to Berend Post berend.post@it-university.nl

Question 897

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

Question 898

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- ☐ The same value.
- ☐ Greater value.
- ☒ Lesser value.
- ☐ Prior audit reports are not relevant.

Explanation:

Explanation:

Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

Question 899

Electromagnetic emissions from a terminal represent an exposure because they:

- ☐ affect noise pollution.
- ☐ disrupt processor functions.
- ☐ produce dangerous levels of electric current.
- ☒ can be detected and displayed.

Explanation:

Explanation:

Emissions can be detected by sophisticated equipment and displayed, thus giving unauthorized person access to data. They should not cause disruption of CPUs or effect noise pollution.

Licensed to Berend Post berend.post@it-university.nl

Question 900

Which of the following is one most common way that spyware is distributed?

- ☒ as a trojan horse.
- ☐ as a virus.
- ☐ as an Adware.
- ☐ as a device driver.
- ☐ as a macro.
- ☐ None of the choices.

Explanation:

Explanation:

One of the most common ways that spyware is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads off the Web or a peer-to-peer file-trading network. When the user installs the software, the spyware is installed alongside.

Question 901

The technique of rummaging through commercial trash to collect useful business information is known as:

- ☒ Information diving
- ☐ Intelligence diving
- ☐ Identity diving
- ☐ System diving
- ☐ Program diving
- ☐ None of the choices.

Explanation:

Explanation:

Dumpster diving in the form of information diving describes the practice of rummaging through commercial trash to find useful information such as files, letters, memos, passwords ...etc.

Question 902

An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

- ☒ An application-level gateway
- ☐ A remote access server
- ☐ A proxy server
- ☐ Port scanning

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

An application-level gateway is the best way to protect against hacking because it can define with detail rules that describe the type of user or connection that is or is not permitted, it analyzes in detail each package, not only in layers one through four of the OSI model but also layers five through seven, which means that it reviews the commands of each higher-level protocol (HTTP, FTP, SNMP, etc.). For a remote access server, there is a device (server) that asks for a username and password before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet creating security exposure. Proxy servers can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program. Port scanning works when there is a very specific task to complete, but not when trying to control what comes from the Internet, or when all the ports available need to be controlled. For example, the port for Ping (echo request) could be blocked and the IP addresses would be available for the application and browsing, but would not respond to Ping.

Question 903

The MOST important function of a business continuity plan is to:

- ☒ ensure that the critical business functions can be recovered
- ☐ provide procedures for evaluating tests of the business continuity plan
- ☐ provide a schedule of events that has to occur if there is a disaster
- ☐ ensure that all business functions are restored

Question 904

Using the OSI reference model, what layer(s) is/are used to encrypt data?

- ☐ transport layer
- ☐ Session layer
- ☒ Session and transport layers
- ☐ Data link layer

Explanation:

Explanation:

User applications often encrypt and encapsulate data using protocols within the OSI session layer or farther down in the transport layer.

Licensed to Berend Post berend.post@it-university.nl

Question 905

In a decentralized organization, the selection and purchase of IS products is acceptable as long as which of the following conditions exists?

- ☐ The same operating system is used throughout the organization.
- ☐ Various offices are independent and exchange data on an occasional basis.
- ☒ Acquired items are consistent with the organization's short- and long-term IS strategy plans.
- ☐ Managers undertake a full cost-benefit analysis before deciding what to purchase.

Question 906

To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

- ☒ during data preparation.
- ☐ in transit to the computer.
- ☐ between related computer runs.
- ☐ during the return of the data to the user department.

Explanation:

Explanation:

During data preparation is the best answer, because it establishes control at the earliest point.

Question 907

Which of the following provides the GREATEST assurance of message authenticity?

- ☐ The prehash code is derived mathematically from the message being sent.
- ☒ The prehash code is encrypted using the sender's private key.
- ☐ The prehash code and the message are encrypted using the secret key.
- ☐ The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Explanation:

Explanation: Encrypting the prehash code using the sender's private key provides assurance of the authenticity of the message. Mathematically deriving the prehash code provides integrity to the message. Encrypting the prehash code and the message using the secretkey provides confidentiality.

Licensed to Berend Post berend.post@it-university.nl

Question 908

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

-The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.

-The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his/her attention.

-The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The basis of an organization's disaster recovery plan is to reestablish live processing at an alternative site where a similar, but not identical, hardware configuration is already established. An IS auditor should:

- ☐ take no action as the lack of a current plan is the only significant finding.
- ☐ recommend that the hardware configuration at each site is identical.
- ☒ perform a review to verify that the second configuration can support live processing.
- ☐ report that the financial expenditure on the alternative site is wasted without an effective plan.

Explanation:

Explanation:

An IS auditor does not have a finding unless it can be shown that the alternative hardware cannot support the live processing system. Even though the primary finding is the lack of a proven and communicated disaster recovery plan, it is essential that this aspect of recovery is included in the audit. If it is found to be inadequate, the finding will materially support the overall audit opinion. It is certainly not appropriate to take no action at all, leaving this important factor untested. Unless it is shown that the alternative site is inadequate, there can be no comment on the expenditure, even if this is considered a proper comment for the IS auditor to make. Similarly, there is no need for the configurations to be identical. The alternative site could actually exceed the recovery requirements if it is also used for other work, such as other processing or systems development and testing. The only proper course of action at this point would be to find out if the recovery site can actually cope with a recovery.

Licensed to Berend Post berend.post@it-university.nl

Question 909

In an annual audit cycle, the audit of an organization's IT department resulted in many findings. Which of the following would be the MOST important consideration when planning the next audit?

- ☐ Limiting the review to the deficient areas
- ☐ Verifying that all recommendations have been implemented
- ☐ Postponing the review until all of the findings have been rectified
- ☒ Following up on the status of all recommendations

Question 910

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

- ☐ Restricting evidence access to professionally certified forensic investigators
- ☐ Engaging an independent third party to perform the forensic investigation
- ☐ Performing investigative procedures on the original hard drives rather than images of the hard drives
- ☒ Documenting evidence handling by personnel throughout the forensic investigation

Question 911

After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?

- ☒ Perform an integral review of the recovery tasks.
- ☐ Broaden the processing capacity to gain recovery time.
- ☐ Make improvements in the facility's circulation structure.
- ☐ increase the amount of human resources involved in the recovery.

Explanation:

Explanation:

Performing an exhaustive review of the recovery tasks would be appropriate to identify the way these tasks were performed, identify the time allocated to each of the steps required to accomplish recovery, and determine where adjustments can be made. Choices B, C and D could be actions after the described review has been completed.

Licensed to Berend Post berend.post@it-university.nl

Question 912

Which of the following is the MOST reliable network connection medium in an environment where there is strong electromagnetic interference?

- ☐ Coaxial cable
- ☒ Fiber optic cable
- ☐ Shielded twisted-pair cable
- ☐ Wireless link

Question 913

Pretexting is an act of:

- ☐ DoS
- ☒ social engineering
- ☐ eavedropping
- ☐ soft coding
- ☐ hard coding
- ☐ None of the choices.

Explanation:

Explanation:

Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action and is usually done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information.

Question 914

What should be the information security manager's MOST important consideration when planning a disaster recovery test?

- ☐ Stakeholder notification procedures
- ☐ Organization-wide involvement
- ☒ Impact to production systems
- ☐ Documented escalation processes

Question 915

Which of the following is a ITU-T standard protocol suite for packet switched wide area network communication?

- ☐ Point-to-point protocol
- ☒ X.25
- ☐ Frame Relay
- ☐ ISDN

Explanation:

Licensed to Berend Post berend.post@it-university.nl

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

For your exam you should know below information about WAN Technologies:

The following answers are incorrect:

Point-to-point protocol - PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server.

Frame Relay - The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

ISDN -Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission. Same copper telephone wire is used. Provide digital point-to-point circuit switching medium.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

Question 916

A hot site should be implemented as a recovery strategy when the:

- ☒ disaster tolerance is low.
- ☐ recovery point objective (RPO) is high.
- ☐ recovery time objective (RTO) is high.
- ☐ disaster tolerance is high.

Explanation:

Explanation:

Disaster tolerance is the time gap during which the business can accept nonavailability of IT facilities. If this time gap is low, recovery strategies that can be implemented within a short period of time, such as a hot site, should be used. The RPO is the earliest point in time at which it is acceptable to recover the data. A high RPO means that the process can wait for a longer time. In such cases, other recovery alternatives, such as warm or cold sites, should be considered. A high RTO means that additional time would be available for the recovery strategy, thus making other recovery alternatives-such as warm or cold sites- viable alternatives.

 Licensed to Berend Post berend.post@it-university.nl

Question 917

For which of the following applications would rapid recovery be MOST crucial?

- ☒ Point-of-sale system
- ☐ Corporate planning
- ☐ Regulatory reporting
- ☐ Departmental chargeback

Explanation:

Explanation:

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

Question 918

Which of the following would BEST provide executive management with current information on IT-related costs and IT performance indicators?

- ☒ IT dashboard
- ☐ Risk register
- ☐ IT service-management plan
- ☐ Continuous audit reports

Question 919

An organization allows its employees to use personal mobile devices for work. Which of the following would BEST maintain information security without compromising employee privacy?

- ☐ Partitioning the work environment from personal space on devices
- ☐ Preventing users from adding applications
- ☒ Restricting the use of devices for personal purposes during working hours
- ☐ Installing security software on the devices

Question 920

Which of the following reduces the potential impact of social engineering attacks?

- ☐ Compliance with regulatory requirements
- ☐ Promoting ethical understanding
- ☒ Security awareness programs
- ☐ Effective performance incentives

Explanation:

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

Licensed to Berend Post berend.post@it-university.nl

Question 921

When determining the specifications for a server supporting an online application using more than a hundred endpoints, which of the following is the MOST important factor to be considered?

- ☒ High availability of different systems
- ☐ Cost-benefit comparison between the available systems
- ☐ Reputation of the vendors and their customer base
- ☐ Transaction volume estimate during peak periods

Question 922

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of incident response procedures?

- ☐ End users have not completed security awareness training.
- ☒ Senior management is not involved in the incident response process.
- ☐ There is no procedure in place to learn from previous security incidents.
- ☐ Critical incident response events are not recorded in a centralized repository.

Question 923

What must an IS auditor understand before performing an application audit?

- ☐ The potential business impact of application risks.
- ☐ Application risks must first be identified.
- ☒ Relative business processes.
- ☐ Relevant application risks.

Explanation:

Explanation:

An IS auditor must first understand relative business processes before performing an application audit.

Question 924

Which of the following should concern an IS auditor when reviewing security in a client- server environment?

- ☐ Protecting data using an encryption technique
- ☐ Preventing unauthorized access using a diskless workstation
- ☒ The ability of users to access and modify the database directly
- ☐ Disabling floppy drives on the users' machines

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

For the purpose of data security in a client-server environment, an IS auditor should be concerned with the user's ability to access and modify a database directly. This could affect the integrity of the data in the database. Data protected by encryption aid in securing the data. Diskless workstations prevent copying of data into local disks and thus help to maintain the integrity and confidentiality of data. Disabling floppy drives is a physical access control, which helps to maintain the confidentiality of data by preventing it from being copied onto a disk.

Question 925

Which of the following should be the PRIMARY consideration for IT management when selecting a new information security tool that monitors suspicious file access patterns?

- ☐ Integration with existing architecture
- ☐ Ease of support and troubleshooting
- ☐ Data correlation and visualization capabilities
- ☒ Ability to contribute to key performance indicator data

Question 926

Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

- ☐ Peak activity periods for the business
- ☐ Remediation dates included in management responses
- ☐ Availability of IS audit resources
- ☒ Complexity of business processes identified in the audit

Question 927

Applying a digital signature to data traveling in a network provides:

- ☐ confidentiality and integrity.
- ☐ security and nonrepudiation.
- ☒ integrity and nonrepudiation.
- ☐ confidentiality and nonrepudiation.

Explanation:

Explanation:

The process of applying a mathematical algorithm to the data that travel in the network and placing the results of this operation with the hash data is used for controlling data integrity, since any unauthorized modification to this data would result in a different hash. The application of a digital signature would accomplish the non-repudiation of the delivery of the message. The term security is a broad concept and not a specific one. In addition to a hash and a digital signature, confidentiality is applied when an encryption process exists.

Licensed to Berend Post berend.post@it-university.nl

Question 928

Which of the following human resources management practices BEST leads to the detection of fraudulent activity?

- ☐ Background checks
- ☐ Time reporting
- ☐ Employee code of ethics
- ☒ Mandatory time off

Question 929

Which of the following is the MOST important driver when developing an effective information security strategy?

- ☐ Security audit reports
- ☐ Benchmarking reports
- ☒ Information security standards
- ☐ Compliance requirements

Question 930

An advantage of using sanitized live transactions in test data is that:

- ☐ all transaction types will be included.
- ☐ every error condition is likely to be tested.
- ☐ no special routines are required to assess the results.
- ☒ test transactions are representative of live processing.

Explanation:

Explanation:

Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

Question 931

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- ☐ Security incident summaries
- ☐ Vendor best practices
- ☐ CERT coordination center
- ☒ Significant contracts

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets. Vendor best practices provides a basis for evaluating how competitive an enterprise is, while security incident summaries are a source for assessing the vulnerabilities associated with the IT infrastructure. CERT {www.cert.org) is an information source for assessing vulnerabilities within the IT infrastructure.

Question 932

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

- ☒ Gateway
- ☐ Protocol converter
- ☐ Front-end communication processor
- ☐ Concentrator/multiplexor

Explanation:

Explanation:

A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

Question 933

Which of the following methods would BEST ensure that IT strategy is in line with business strategy?

- ☐ Break-even-point analysis
- ☒ IT value analysis
- ☐ Critical path analysis
- ☐ Business impact analysis (BIA)

Question 934

Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability and integrity of data?

- ☐ Secure Sockets Layer (SSL)
- ☐ Intrusion detection system (IDS)
- ☒ Public key infrastructure (PKI)
- ☐ Virtual private network (VPN)

Explanation:

Explanation:

PKI would be the best overall technology because cryptography provides for encryption, digital signatures and non-repudiation controls for confidentiality and reliability. SSL can provide confidentiality. IDS is a detective control. A VPN would provide confidentiality and authentication (reliability).

Licensed to Berend Post berend.post@it-university.nl

Question 935

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

- ☒ digitally signing all e-mail messages.
- ☐ encrypting all e-mail messages.
- ☐ compressing all e-mail messages.
- ☐ password protecting all e-mail messages.

Explanation:

Explanation:

By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able to open the message; however, it would not ensure the authenticity of the sender.

Question 936

An employee of an organization has reported losing a smartphone that contains sensitive information. The BEST step to address this situation should be to:

- ☐ terminate the device connectivity
- ☐ escalated to the user's management
- ☐ disable the user's access to corporate resources
- ☒ remotely wipe the device

Question 937

Which of the following is the MOST important aspect relating to employee termination?

- ☐ The details of employee have been removed from active payroll files.
- ☐ Company property provided to the employee has been returned.
- ☐ User ID and passwords of the employee have been deleted.
- ☒ The appropriate company staff are notified about the termination.

Explanation:

Even though Logical access to information by a terminated employee is possible if the ID and password of the terminated employee has not been deleted this is only one part of the termination procedures. If user ID is not disabled or deleted, it could be possible for the employee without physical access to visit the company's networks remotely and gain access to the information.

Licensed to Berend Post berend.post@it-university.nl

Please note that this can also be seen in a different way: the most important thing to do could also be to inform others of the person's termination, because even if user ID's and passwords are deleted, a terminated individual could simply socially engineer their way back in by calling an individual he/she used to work with and ask them for access. He could intrude on the facility or use other weaknesses to gain access to information after he has been terminated.

By notifying the appropriate company staff about the termination, they would in turn initiate account termination, ask the employee to return company property, and all credentials would be withdrawn for the individual concerned. This answer is more complete than simply disabling account.

It seems harsh and cold when this actually takes place, but too many companies have been hurt by vengeful employees who have lashed out at the company when their positions were revoked for one reason or another. If an employee is disgruntled in any way, or the termination is unfriendly, that employee's accounts should be disabled right away, and all passwords on all systems changed.

For your exam you should know the information below:

Employee Termination Processes

Employees join and leave organizations every day. The reasons vary widely, due to retirement, reduction in force, layoffs, termination with or without cause, relocation to another city, career opportunities with other employers, or involuntary transfers. Terminations may be friendly or unfriendly and will need different levels of care as a result.

Friendly Terminations

Regular termination is when there is little or no evidence or reason to believe that the termination is not agreeable to both the company and the employee. A standard set of procedures, typically maintained by the human resources department, governs the dismissal of the terminated employee to ensure that company property is returned, and all access is removed. These procedures may include exit interviews and return of keys, identification cards, badges, tokens, and cryptographic keys. Other property, such as laptops, cable locks, credit cards, and phone cards, are also collected. The user manager notifies the security department of the termination to ensure that access is revoked for all platforms and facilities. Some facilities choose to immediately delete the accounts, while others choose to disable the accounts for a policy defined period, for example, 30 days, to account for changes or extensions in the final termination date. The termination process should include a conversation with the departing associate about their continued responsibility for confidentiality of information.

Unfriendly Terminations

Unfriendly terminations may occur when the individual is fired, involuntarily transferred, laid off, or when the organization has reason to believe that the individual has the means and intention to

Licensed to Berend Post berend.post@it-university.nl

potentially cause harm to the system. Individuals with technical skills and higher levels of access, such as the systems administrators, computer programmers, database administrators, or any individual with elevated privileges, may present higher risk to the environment. These individuals could alter files, plant logic bombs to create system file damage at a future date, or remove sensitive information. Other disgruntled users could enter erroneous data into the system that may not be discovered for several months. In these situations, immediate termination of systems access is warranted at the time of termination or prior to notifying the employee of the termination. Managing the people aspect of security, from pre-employment to postemployment, is critical to ensure that trustworthy, competent resources are employed to further the business objectives that will protect company information. Each of these actions contributes to preventive, detective, or corrective personnel controls.

The following answers are incorrect:

The other options are less important.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 99

Harris, Shun (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 129). McGraw-Hill. Kindle Edition.

Question 938

Which of the following is the BEST source for describing the objectives of an organization's information systems?

- ☐ Business process owners
- ☐ End users
- ☐ IT management
- ☒ Information security management

Question 939

Both statistical and nonstatistical sampling techniques:

- ☒ permit the auditor to quantify the probability of error.
- ☐ permit the auditor to quantify and fix the level of risk.
- ☐ require judgment when defining population characteristics.
- ☐ provide each item an equal opportunity of being selected.

Licensed to Berend Post berend.post@it-university.nl

Question 940

An IS auditor should carefully review the functional requirements in a system-development project to ensure that the project is designed to:

- ☒ Meet business objectives
- ☐ Enforce data security
- ☐ Be culturally feasible
- ☐ Be financially feasible

Explanation:

Explanation:

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

Question 941

Which of the following would BEST help to support an auditor's conclusion about the effectiveness of an implemented data classification program?

- ☐ Detailed data classification scheme
- ☐ Access rights provisioned according to scheme
- ☒ Business use cases and scenarios
- ☐ Purchase of information management tools

Question 942

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions.

Licensed to Berend Post berend.post@it-university.nl

Question 943

Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

- ☒ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Explanation:

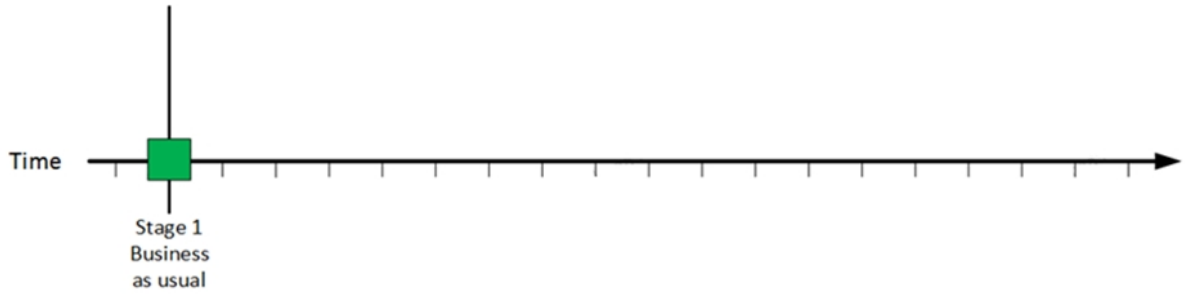
Explanation:

A recovery point objective, or "RPO", is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. For instance, if the RPO is set to four hours, then in practice, off-site mirrored backups must be continuously maintained – a daily off-site backup on tape will not suffice. Care must be taken to avoid two common mistakes around the use and definition of RPO. Firstly, BC staff use business impact analysis to determine RPO for each service – RPO is not determined by the existent backup regime. Secondly, when any level of preparation of off-site data is required, rather than at the time the backups are offsite, the period during which data is lost very often starts near the time of the beginning of the work to prepare backups which are eventually offsite.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

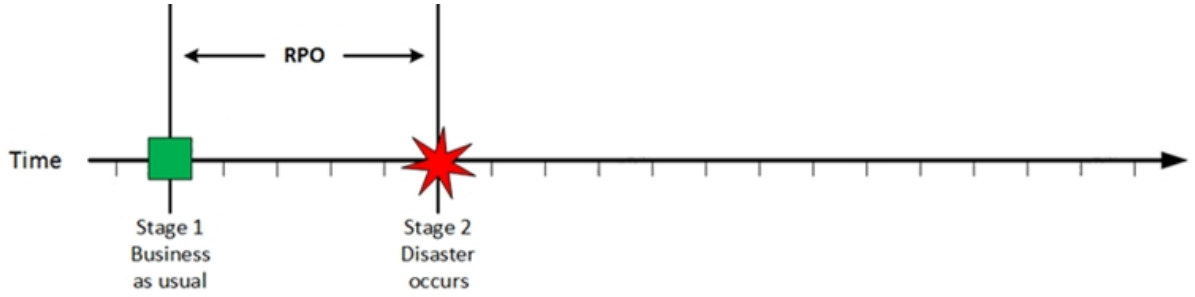


At this stage all systems are running production and working correctly.

Licensed to Berend Post berend.post@it-university.nl

Stage 2: Disaster occurs

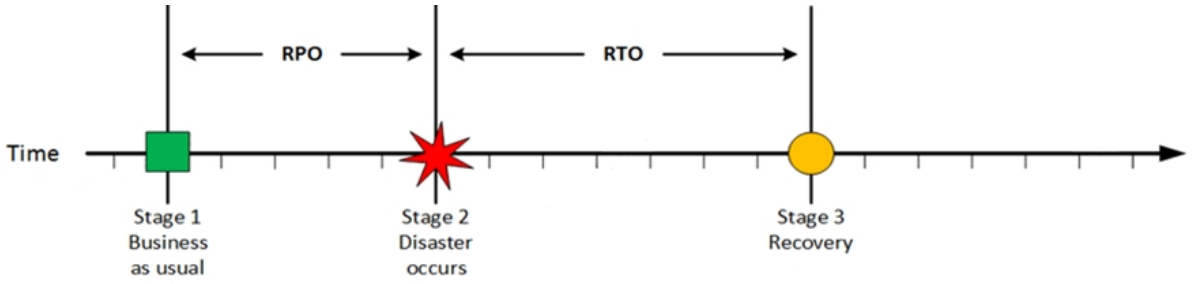
Disaster Occurs



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

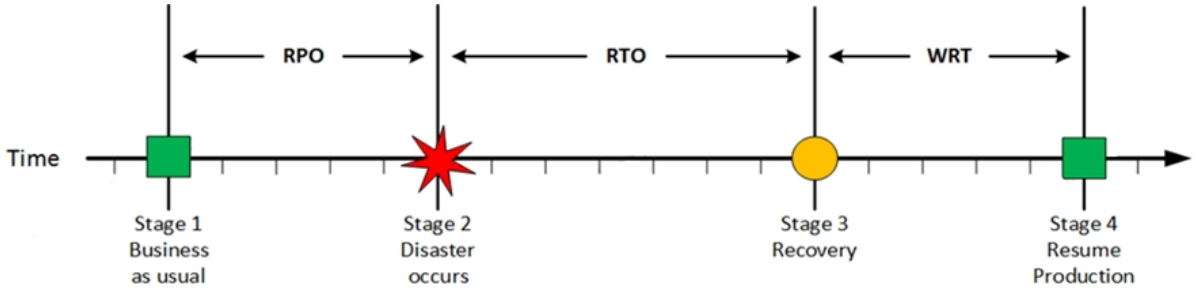


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

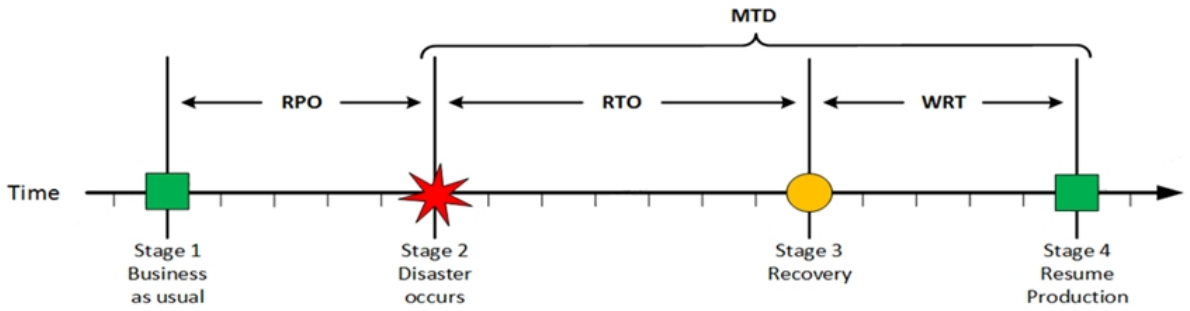
Resume Production

Licensed to Berend Post berend.post@it-university.nl



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Licensed to Berend Post berend.post@it-university.nl

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

References:

CISA review manual 2014 page number 284

http://en.wikipedia.org/wiki/Recovery_point_objective

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 944

When an employee is terminated from service, the MOST important action is to:

- ☐ hand over all of the employee's files to another designated employee.
- ☐ complete a backup of the employee's work.
- ☐ notify other employees of the termination.
- ☒ disable the employee's logical access.

Explanation:

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

Licensed to Berend Post berend.post@it-university.nl

Question 945

A structured walk-through test of a disaster recovery plan involves:

- ☐ representatives from each of the functional areas coming together to go over the plan.
- ☒ all employees who participate in the day-to-day operations coming together to practice executing the plan.
- ☐ moving the systems to the alternate processing site and performing processing operations.
- ☐ distributing copies of the plan to the various functional areas for review.

Explanation:

Explanation:

A structured walk-through test of a disaster recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required. Choice B is a simulation test to prepare and train the personnel who will be required to respond to disasters and disruptions. Choice C is a form of parallel testing to ensure that critical systems will perform satisfactorily in the alternate site. Choice D is a checklist test.

Question 946

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off?

- ☐ Employee security awareness training
- ☐ Administrator alerts
- ☒ Screensaver passwords
- ☐ Close supervision

Explanation:

Explanation:

Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.

Question 947

What is essential for the IS auditor to obtain a clear understanding of network management?

- ☐ Security administrator access to systems
- ☐ Systems logs of all hosts providing application services
- ☒ A graphical map of the network topology
- ☐ Administrator access to systems

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management.

Question 948

Which procedure provides the GREATEST assurance that corrective action to an audit report has been taken?

- ☒ Performing subsequent audit tests to verify resolution of the deficiencies
- ☐ Inquiring about the current status of the recommendation
- ☐ Reporting to the audit committee or the board of directors concerning specific action taken or lack thereof
- ☐ Requesting a written management reply to the audit report, identifying corrective action for each deficiency

Question 949

Which of the following would be MOST useful to an information security manager when conducting a post-incident review of an attack?

- ☐ Details from intrusion detection system logs
- ☒ Method of operation used by the attacker
- ☐ Cost of the attack to the organization
- ☐ Location of the attacker

Question 950

A penetration test performed as part of evaluating network security:

- ☐ provides assurance that all vulnerabilities are discovered.
- ☐ should be performed without warning the organization's management.
- ☒ exploits the existing vulnerabilities to gain unauthorized access.
- ☐ would not damage the information assets when performed at network perimeters.

Explanation:

Explanation:

Penetration tests are an effective method of identifying real-time risks to an information processing environment. They attempt to break into a live site in order to gain unauthorized access to a system. They do have the potential for damaging information assets or misusing information because they mimic an experienced hacker attacking a live system. On the other hand, penetration tests do not provide assurance that all vulnerabilities are discovered because they are based on a limited number of procedures. Management should provide consent for the test to avoid false alarms to IT personnel or to law enforcement bodies.

Licensed to Berend Post berend.post@it-university.nl

Question 951

Multiple invoices are usually received for individual purchase orders, since purchase orders require staggered delivery dates. Which of the following is the BEST audit technique to test for duplicate payments?

- ☒ Run the data on the software programs used to process supplier payments.
- ☐ Use generalized audit software on the invoice transaction file.
- ☐ Run the data on the software programs used to process purchase orders.
- ☐ Use generalized audit software on the purchase order transaction file.

Question 952

Which of the following is a software application that pretend to be a server on the Internet and is not set up purposely to actively protect against break-ins?

- ☐ Bastion host
- ☒ Honey pot
- ☐ Dual Homed
- ☐ Demilitarize Zone (DMZ)

Explanation:

A Honey pot is a software application or system that pretends to be a normal server on the internet and it is not set up actively protect against all break-ins. In purpose, some of the updates, patches, or upgrades are missing.

You then monitor the honey pot to learn from the offensive side.

There are two types of honey pot:

High-interaction Honey pots – Essentially gives hacker a real environment to attack. High-interaction honey pots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. According to recent research into high-interaction honey pot technology, by employing virtual machines, multiple honey pots can be hosted on a single physical machine. Therefore, even if the honey pot is compromised, it can be restored more quickly. In general, high-interaction honey pots provide more security by being difficult to detect, but they are highly expensive to maintain. If virtual machines are not available, one honey pot must be maintained for each physical computer, which can be exorbitantly expensive. Example: Honey net.

Low interaction – Emulate production environment and therefore, provide more limited information. Low-interaction honey pots simulate only the services frequently requested by attackers. Since they consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyed.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Bastion host - On the Internet, a bastion host is the only host computer that a company allows to be addressed directly from the public network and that is designed to screen the rest of its network from security exposure. DMZ or Demilitarize Zone In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Dual Homed - Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures for implementing preventive security.

Dual-Homed - An example of dual-homed devices are enthusiast computing motherboards that incorporate dual Ethernet network interface cards or a firewall with two network interface cards. One facing the external network and one facing the internal network.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

http://searchsecurity.techtarget.com/definition/bastion-hosthttp://searchsecurity.techtarget.com/definition/DMZ

http://en.wikipedia.org/wiki/Honeypot_%28computing%29

http://en.wikipedia.org/wiki/Dual-homed

Question 953

Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

- ☐ format string vulnerabilities
- ☐ integer overflow
- ☒ code injection
- ☐ command injection
- ☐ None of the choices.

Explanation:

Explanation:

Code injection is a technique to introduce code into a computer program or system by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs.

Licensed to Berend Post berend.post@it-university.nl

Question 954

Which of the following measures can effectively minimize the possibility of buffer overflows?

- ☒ Sufficient bounds checking
- ☐ Sufficient memory
- ☐ Sufficient processing capability
- ☐ Sufficient code injection
- ☐ None of the choices

Explanation:

Explanation:

Buffer overflows may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits. Sufficient bounds checking by either the programmer or the compiler can prevent buffer overflows.

Question 955

The use of symmetric key encryption controls to protect sensitive data transmitted over a communications network requires that:

- ☒ primary keys for encrypting the data be stored in encrypted form.
- ☐ encryption keys be changed only when a compromise is detected at both ends.
- ☐ encryption keys at one end be changed on a regular basis.
- ☐ public keys be stored in encrypted form.

Question 956

Which of the following controls would provide the GREATEST assurance of database integrity?

- ☐ Audit log procedures
- ☒ Table link/reference checks
- ☐ Query/table access time checks
- ☐ Rollback and roll forward database features

Explanation:

Explanation:

Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database), and thus provides the greatest assurance of database integrity. Audit log procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and roll forward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being

Licensed to Berend Post berend.post@it-university.nl

processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

Question 957

An IS auditor performing a review of an application's controls would evaluate the:

- ☐ efficiency of the application in meeting the business processes.
- ☒ impact of any exposures discovered.
- ☐ business processes served by the application.
- ☐ application's optimization.

Explanation:

Explanation:

An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

Question 958

Which of the following would be the BEST population to take a sample from when testing program changes?

- ☐ Test library listings
- ☐ Source program listings
- ☐ Program change requests
- ☒ Production library listings

Explanation:

Explanation:

The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational data. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

Licensed to Berend Post berend.post@it-university.nl

Question 959

After the release of an application system, an IS auditor wants to verify that the system is providing value to the organization. The auditor's BEST course of action would be to:

- ☐ review the results of compliance testing.
- ☐ quantify improvements in client satisfaction.
- ☐ confirm that risk has declined since the application system release.
- ☒ perform a gap analysis against the benefits defined in the business case.

Question 960

A grants management system is used to calculate grant payments. Once per day, a batch interface extracts grant amounts and payee details from this system for import into the finance system so payments can be made overnight. Which of the following controls provides the GREATEST assurance and completeness of the imported payments?

- ☐ Performing monthly bank reconciliations in a timely manner
- ☐ Restricting access to the grants and finance systems
- ☐ Reviewing transaction logs for anomalies
- ☒ Reconciling data from both systems

Question 961

The PRIMARY objective of an audit of IT security policies is to ensure that:

- ☐ they are distributed and available to all staff.
- ☒ security and control policies support business and IT objectives.
- ☐ there is a published organizational chart with functional descriptions.
- ☐ duties are appropriately segregated.

Explanation:

Explanation:

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

Licensed to Berend Post berend.post@it-university.nl

Question 962

What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

- ☒ Malicious code could be spread across the network
- ☐ VPN logon could be spoofed
- ☐ Traffic could be sniffed and decrypted
- ☐ VPN gateway could be compromised

Explanation:

Explanation:

VPN is a mature technology; VPN devices are hard to break. However, when remote access is enabled, malicious code in a remote client could spread to the organization's network. Though choices B, C and D are security risks, VPN technology largely mitigates these risks.

Question 963

A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

- ☐ reasonableness check.
- ☐ parity check.
- ☒ redundancy check.
- ☐ check digits.

Explanation:

Explanation:

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data.

Question 964

Which of the following is the BEST type of program for an organization to implement to aggregate, correlate and store different log and event files, and then produce weekly and monthly reports for IS auditors?

- ☐ A security information event management (SIEM) product
- ☐ An open-source correlation engine
- ☒ A log management tool
- ☐ An extract, transform, load (ETL) system

Explanation:

Explanation:

A log management tool is a product designed to aggregate events from many log files (with distinct formats and from different sources), store them and typically correlate them offline to produce many reports (e.g., exception reports showing different statistics including anomalies and suspicious

Licensed to Berend Post berend.post@it-university.nl

activities), and to answer time-based queries (e.g., how many users have entered the system between 2 a.m. and 4 a.m. over the past three weeks?). A SIEM product has some similar features. It correlates events from log files, but does it online and normally is not oriented to storing many weeks of historical information and producing audit reports. A correlation engine is part of a SIEM product. It is oriented to making an online correlation of events. An extract, transform, load (ETL) is part of a business intelligence system, dedicated to extracting operational or production data, transforming that data and loading them to a central repository (data warehouse or data mart); an ETL does not correlate data or produce reports, and normally it does not have extractors to read log file formats.

Question 965

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

- ☐ Technology risks must be mitigated.
- ☐ Management requires regular reports.
- ☒ The environment changes constantly.
- ☐ The current threat levels are being assessed.

Question 966

Which of the following scenarios would enable a forensic investigation?

- ☒ The suspected computer was rebooted, and the evidence log file was converted to a readable format for further analysis.
- ☐ The incident response team prepared a final report for the forensic investigator and deleted the original file securely to avoid further damage.
- ☐ The media in question was preserved using imaging, and chain of custody was documented according to the organization's incident response plan.
- ☐ Incident response team members extracted the logs showing the suspicious activity and added their notes before submitting for investigation.

Question 967

During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

- ☐ Postpone the audit until the agreement is documented
- ☐ Report the existence of the undocumented agreement to senior management
- ☒ Confirm the content of the agreement with both departments
- ☐ Draft a service level agreement (SLA) for the two departments

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

An IS auditor should first confirm and understand the current practice before making any recommendations. The agreement can be documented after it has been established that there is an agreement in place. The fact that there is not a written agreement does not justify postponing the audit, and reporting to senior management is not necessary at this stage of the audit. Drafting a service level agreement (SLA) is not the IS auditor's responsibility.

Question 968

In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the:

- ☒ major IT initiatives.
- ☐ links to operational tactical plans.
- ☐ allocation of IT staff
- ☐ project management methodologies used.

Question 969

Implementing a strong password policy is part of an organization's information security strategy for the year. A business unit believes the strategy may adversely affect a client's adoption of a recently developed mobile application and has decided not to implement the policy. Which of the following would be the information security manager's BEST course of action?

- ☒ Analyze the risk and impact of not implementing the policy
- ☐ Develop and implement a password policy for the mobile application
- ☐ Escalate non-implementation of the policy to senior management
- ☐ Benchmark with similar mobile applications to identify gaps

Question 970

As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

- ☐ Organizational risks, such as single point-of-failure and infrastructure risk
- ☐ Threats to critical business processes
- ☒ Critical business processes for ascertaining the priority for recovery
- ☐ Resources required for resumption of business

Explanation:

Explanation:

The identification of the priority for recovering critical business processes should be addressed first. Organizational risks should be identified next, followed by the identification of threats to critical business processes. Identification of resources for business resumption will occur after the tasks mentioned.

Licensed to Berend Post berend.post@it-university.nl

Question 971

A risk analysis for a new system is being performed. For which of the following is business knowledge MORE important than IT knowledge?

- ☐ Vulnerability analysis
- ☒ Cost-benefit analysis
- ☐ Impact analysis
- ☐ Balanced scorecard

Question 972

Which of the following external entities would provide the BEST guidance to an organization facing advanced attacks?

- ☒ Recognized threat intelligence communities
- ☐ Open-source reconnaissance
- ☐ Disaster recovery consultants widely endorsed in industry forums
- ☐ Incident response experts from highly regarded peer organizations

Question 973

Which of the following data validation control validates input data against predefined range values?

- ☒ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Explanation:

In the Range Check control data should not exceed a predefined range of values

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Licensed to Berend Post berend.post@it-university.nl

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Licensed to Berend Post berend.post@it-university.nl

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 215

Question 974

The optimum business continuity strategy for an entity is determined by the:

- ☐ lowest downtime cost and highest recovery cost.
- ☒ lowest sum of downtime cost and recovery cost.
- ☐ lowest recovery cost and highest downtime cost.
- ☐ average of the combined downtime and recovery cost.

Explanation:

Explanation:

Both costs have to be minimized, and the strategy for which the costs are lowest is the optimum strategy. The strategy with the highest recovery cost cannot be the optimum strategy. The strategy with the highest downtime cost cannot be the optimum strategy. The average of the combined downtime and recovery cost will be higher than the lowest combined cost of downtime and recovery.

Licensed to Berend Post berend.post@it-university.nl

Question 975

Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the BEST way to address this situation?

- ☐ Data modeling
- ☐ Data visualization
- ☐ Data mining
- ☒ Data purging

Question 976

Reverse proxy technology for web servers should be deployed if:

- ☒ http servers' addresses must be hidden.
- ☐ accelerated access to all published pages is required.
- ☐ caching is needed for fault tolerance.
- ☐ bandwidth to the user is limited.

Explanation:

Explanation:

Reverse proxies are primarily designed to hide physical and logical internal structures from outside access. Complete URLs or URIs can be partially or completely redirected without disclosing which internal or DMZ server is providing the requested data. This technology might be used if a trade-off between security, performance and costs has to be achieved. Proxy servers cache some data but normally cannot cache all pages to be published because this depends on the kind of information the web servers provide. The ability to accelerate access depends on the speed of the back-end servers, i.e., those that are cached. Thus, without making further assumptions, a gain in speed cannot be assured, but visualization and hiding of internal structures can. If speed is an issue, a scale- out approach (avoiding adding additional delays by passing firewalls, involving more servers, etc.) would be a better solution. Due to the limited caching option, reverse proxies are not suitable for enhancing fault tolerance. User requests that are handled by reverse proxy servers are using exactly the same bandwidth as direct requests to the hosts providing the data.

Question 977

A comprehensive IS audit policy should include guidelines detailing what involvement the internal audit team should have?

- ☐ in the development and coding of major OS applications.
- ☐ in the acquisition and maintenance of major WEB applications.
- ☐ in the human resource management cycle of the application development project.
- ☒ in the development, acquisition, conversion, and testing of major applications.
- ☐ None of the choices.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The audit policy should include guidelines detailing what involvement internal audit will have in the development, acquisition, conversion, and testing of major applications. Such a policy must be approved by top management for it to be effective.

Question 978

When following up on a data breach, an IS auditor finds a system administrator may have compromised the chain of custody. Which of the following should the system administrator have done FIRST to preserve the evidence?

- ☐ Perform forensic discovery
- ☐ Notify key stakeholders
- ☒ Quarantine the system
- ☐ Notify the incident response team

Question 979

Which of the following should be an IS auditor's FIRST action when assessing the risk associated with unstructured data?

- ☐ Implement strong encryption for unstructured data.
- ☐ Implement user access controls to unstructured data.
- ☐ Identify repositories of unstructured data.
- ☒ Identify appropriate tools for data classification.

Question 980

An IS auditor is reviewing IT policies and found that most policies have not been reviewed in over 3 years. The MOST significant risk is that the policies do not reflect:

- ☒ current legal requirements.
- ☐ the vision of the CEO.
- ☐ the mission of the organization.
- ☐ current industry best practices.

Question 981

Which of the following database model allow many-to-many relationships in a tree-like structure that allows multiple parents?

- ☐ Hierarchical database model
- ☒ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

Hierarchical database model

Network model

Relational model

Object-relational database models

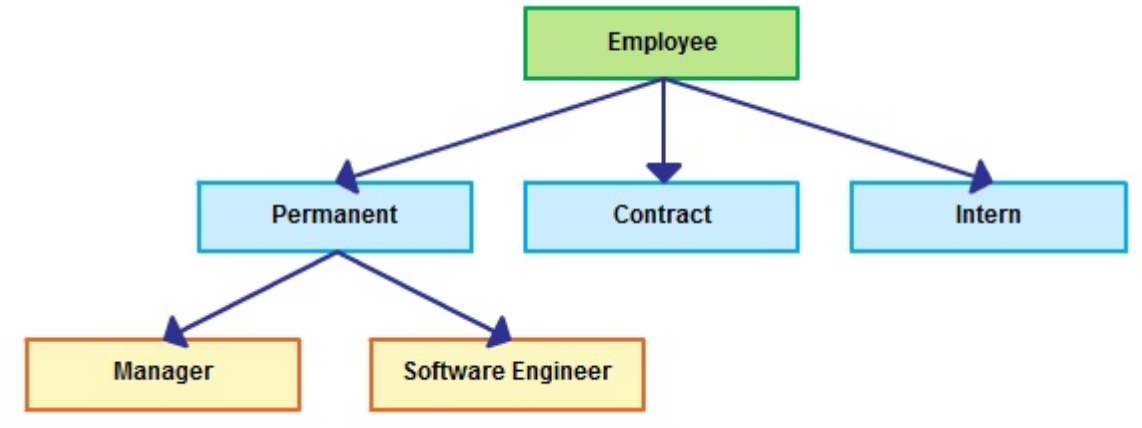
Hierarchical database model

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model

Licensed to Berend Post berend.post@it-university.nl



Network database model

The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

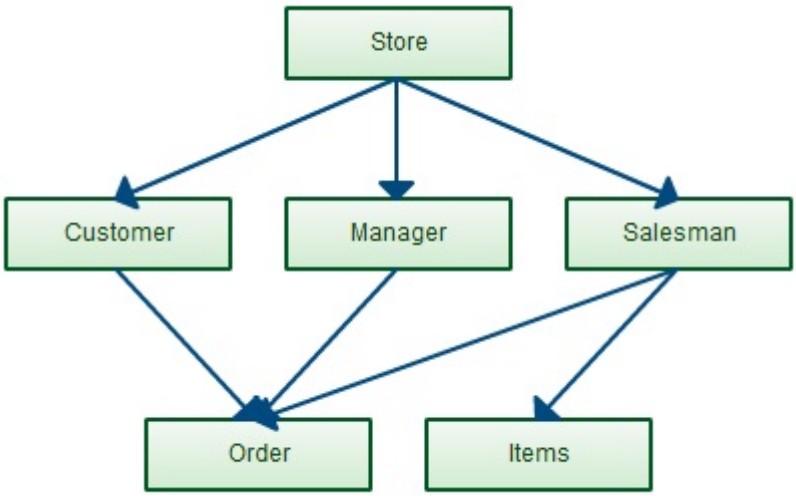
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.

Network Database model

Licensed to Berend Post berend.post@it-university.nl



Relational database model

In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

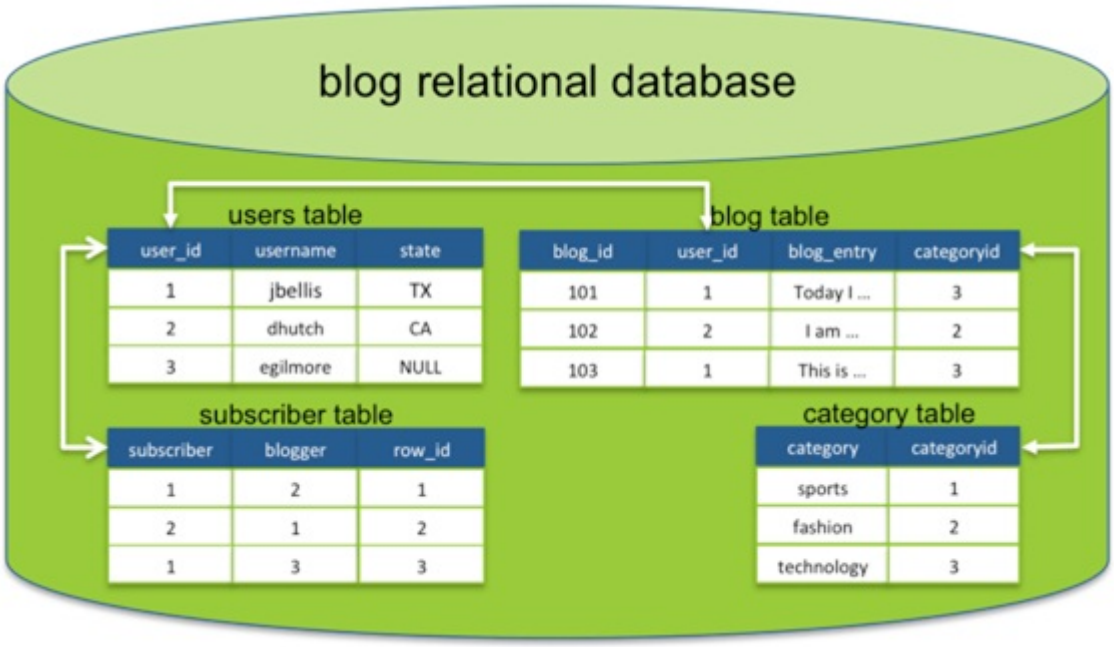
In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.

Relational database model

Licensed to Berend Post berend.post@it-university.nl



Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

Relational model- In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are

Licensed to Berend Post berend.post@it-university.nl

OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 254

Question 982

During an IS audit, one of your auditor has observed that some of the critical servers in your organization can be accessed ONLY by using shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

- ☐ Password sharing
- ☒ Accountability
- ☐ Shared account management
- ☐ Difficulty in auditing shared account

Explanation:

The keyword PRIMARY is used in the question. Accountability should be the primary concern if critical servers can be accessed only by using shared user id and password. It would be very difficult to track the changes done by employee on critical server.

For your exam you should know the information below:

Accountability

Ultimately one of the drivers behind strong identification, authentication, auditing and session management is accountability. Accountability is fundamentally about being able to determine who or what is responsible for an action and can be held responsible. A closely related information assurance topic is non-repudiation. Repudiation is the ability to deny an action, event, impact or result. Non-repudiation is the process of ensuring a user may not deny an action. Accountability relies heavily on non-repudiation to ensure users, processes and actions

may be held responsible for impacts.

The following contribute to ensuring accountability of actions:

Strong identification

Strong authentication

User training and awareness

Comprehensive, timely and thorough monitoring

Licensed to Berend Post berend.post@it-university.nl

Accurate and consistent audit logs

Independent audits

Policies enforcing accountability

Organizational behavior supporting accountability

The following answers are incorrect:

The other options are also valid concern. But the primary concern should be accountability.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 328 and 329

Official ISC2 guide to CISSP CBK 3rd Edition Page number 114

Question 983

An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

- ☒ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Explanation:

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

Question 984

An information security manager has developed a strategy to address new information security risks resulting from recent changes in the business. Which of the following would be MOST important to include when presenting the strategy to senior management?

- ☒ The impact of organizational changes on the security risk profile
- ☐ The costs associated with business process changes
- ☐ Results of benchmarking against industry peers
- ☐ Security controls needed for risk mitigation

Licensed to Berend Post berend.post@it-university.nl

Question 985

Which of the following layer of an enterprise data flow architecture is concerned with basic data communication?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☒ Internet/Intranet layer
- ☐ Data access layer

Explanation:

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Licensed to Berend Post berend.post@it-university.nl

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and

Licensed to Berend Post berend.post@it-university.nl

context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Licensed to Berend Post berend.post@it-university.nl

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 986

Which of the following should be an IS auditor's BEST recommendation to prevent installation of unlicensed software on employees' company-provided devices?

- ☒ Enforce audit logging of software installation activities.
- ☐ Restrict software installation authority to administrative users only.
- ☐ Implement software blacklisting.
- ☐ Remove unlicensed software from end-user devices.

Question 987

Software is considered malware based on:

- ☒ the intent of the creator.
- ☐ its particular features.
- ☐ its location.
- ☐ its compatibility.
- ☐ None of the choices.

Explanation:

Explanation:

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Software is considered malware based on the intent of the creator rather than any particular features. It includes computer viruses, worms, trojan horses, spyware, adware, and other malicious and unwanted software.

Licensed to Berend Post berend.post@it-university.nl

Question 988

While planning a review of IT governance, the IS auditor is MOST likely to:

- ☒ examine audit committee minutes for IS-related matters and their control.
- ☐ obtain information about the framework of control adopted by management.
- ☐ assess whether business process owner responsibilities are consistent across the organization.
- ☐ review compliance with policies and procedures issued by the board of directors.

Question 989

When conducting a review of security incident management, an IS auditor found there are no defined escalation processes. All incidents are managed by the service desk. Which of the following should be the auditor's PRIMARY concern?

- ☐ Inefficient use of service desk resources
- ☒ Management's lack of high impact incidents
- ☐ Delays in resolving low priority trouble tickets
- ☐ Management's inability to follow up on incident resolution

Question 990

Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

- ☐ Ensuring that invoices are paid to the provider
- ☐ Participating in systems design with the provider
- ☐ Renegotiating the provider's fees
- ☒ Monitoring the outsourcing provider's performance

Explanation:

Explanation:

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

Licensed to Berend Post berend.post@it-university.nl

Question 991

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

- ☐ Reasonableness check
- ☐ Parity check
- ☒ Redundancy check
- ☐ Check digits

Explanation:

Explanation:

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission.

Check digits detect transposition and transcription errors.

Question 992

Which of the following is the BEST data integrity check?

- ☐ Counting the transactions processed per day
- ☐ Performing a sequence check
- ☒ Tracing data back to the point of origin
- ☐ Preparing and running test data

Question 993

Which of the following could be used to evaluate the effectiveness of IT operations?

- ☐ Total cost of ownership
- ☐ Net present value
- ☒ Balanced scorecard
- ☐ Internal rate of return

Question 994

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Allowing application programmers to directly patch or change code in production programs increases risk of fraud.

Question 995

Which of the following ACID property ensures that transaction will bring the database from one valid state to another?

- ☐ Atomicity
- ☒ Consistency
- ☐ Isolation
- ☐ Durability

Explanation:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction.[citation needed]

Licensed to Berend Post berend.post@it-university.nl

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

The following were incorrect answers:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

Question 996

During an audit of the logical access control of an ERP financial system an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. These accounts allow access to financial transactions on the ERP. What should the IS auditor do next?

- ☒ Look for compensating controls.
- ☐ Review financial transactions logs.
- ☐ Review the scope of the audit.
- ☐ Ask the administrator to disable these accounts.

Explanation:

Explanation:

The best logical access control practice is to create user IDs for each individual to define accountability. This is possible only by establishing a one-to-one relationship between IDs and individuals. However, if the user IDs are created based on role designations, an IS auditor should first understand the reasons and then evaluate the effectiveness and efficiency of compensating controls. Reviewing transactions logs is not relevant to an audit of logical access control nor is reviewing the

 Licensed to Berend Post berend.post@it-university.nl

scope of the audit relevant. Asking the administrator to disable the shared accounts should not be recommended by an IS auditor before understanding the reasons and evaluating the compensating controls. It is not an IS auditor's responsibility to ask for disabling accounts during an audit.

Question 997

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- ☒ an assessment of the fit of the organization's application portfolio with business objectives.
- ☐ actions to reduce hardware procurement cost.
- ☐ a listing of approved suppliers of IT contract resources.
- ☐ a description of the technical architecture for the organization's network perimeter security.

Explanation:

Explanation:

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail ofa specific technical architecture.

Question 998

The MOST effective control for addressing the risk of piggybacking is:

- ☐ a single entry point with a receptionist.
- ☐ the use of smart cards.
- ☐ a biometric door lock.
- ☒ a deadman door.

Explanation:

Explanation:

Deadman doors are a system of using a pair of (two) doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding areA. This reduces the risk of an unauthorized person following an authorized person through a secured entry (piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

Licensed to Berend Post berend.post@it-university.nl

Question 999

Before implementing controls, management should FIRST ensure that the controls:

- ☒ satisfy a requirement in addressing a risk issue.
- ☐ do not reduce productivity.
- ☐ are based on a cost-benefit analysis.
- ☐ are detective or corrective.

Explanation:

Explanation:

When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

Question 1000

The MOST important reason why an IT risk assessment should be updated on a regular basis is to:

- ☐ utilize IT resources in a cost-effective manner
- ☐ comply with data classification changes
- ☐ comply with risk management policies
- ☒ react to changes in the IT environment

Question 1001

Planning for the implementation of an information security program is MOST effective when it:

- ☐ uses risk-based analysis for security projects.
- ☐ applies technology-driven solutions to identified needs.
- ☐ uses decision trees to prioritize security projects.
- ☒ applies gap analysis to current and future business plans.

Question 1002

Which of the following should be of concern to an IS auditor performing a software audit on virtual machines?

- ☒ Software licensing does not support virtual machines.
- ☐ Software has been installed on virtual machines by privileged users.
- ☐ Multiple users can access critical applications.
- ☐ Applications have not been approved by the CFO.

Licensed to Berend Post berend.post@it-university.nl

Question 1003

The purpose of a mainframe audit is to provide assurance that processes are being implemented as required, the mainframe is operating as it should, security is strong, and that procedures in place are working and are updated as needed. The auditor may accordingly make recommendations for improvement. Which of the following types of audit always takes high priority over the others? (Choose five.)

- ☒ System audit
- ☒ Application audit
- ☒ Software audit
- ☒ License audit
- ☒ Security server audit
- ☐ None of the choices.

Question 1004

Which of the following is the MOST important action in recovering from a cyberattack?

- ☐ Creation of an incident response team
- ☐ Use of cyber forensic investigators
- ☒ Execution of a business continuity plan
- ☐ Filling an insurance claim

Explanation:

Explanation: The most important key step in recovering from cyberattacks is the execution of a business continuity plan to quickly and cost-effectively recover critical systems, processes and data. The incident response team should exist prior to a cyberattack. When a cyberattack is suspected, cyber forensic investigators should be used to set up alarms, catch intruders within the network, and track and trace them over the Internet. After taking the above steps, an organization may have a residual risk that needs to be insured and claimed for traditional and electronic exposures.

Question 1005

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- ☒ Replay
- ☐ Brute force
- ☐ Cryptographic
- ☐ Mimic

Explanation:

Explanation:

Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access. A brute force attack involves feeding the biometric capture device numerous different biometric samples. A cryptographic attack targets the

Licensed to Berend Post berend.post@it-university.nl

algorithm or the encrypted data, in a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user, such as forging a signature or imitating a voice.

Question 1006

What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

- ☐ Update the threat landscape
- ☐ Review the effectiveness of controls
- ☐ Determine operational losses
- ☒ Improve the change control process

Question 1007

A review of an organization's IT portfolio revealed several applications that are not in use. The BEST way to prevent this situation from recurring would be to implement:

- ☐ a formal request for proposal (RFP) process
- ☐ an information asset acquisition policy
- ☒ asset life cycle management
- ☐ business case development procedures

Question 1008

Which of the following is an advantage of prototyping?

- ☐ The finished system normally has strong internal controls.
- ☒ Prototype systems can provide significant time and cost savings.
- ☐ Change control is often less complicated with prototype systems.
- ☐ it ensures that functions or extras are not added to the intended system.

Question 1009

What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

- ☐ Accuracy check
- ☐ Completeness check
- ☒ Reasonableness check
- ☐ Redundancy check

Explanation:

Explanation:

A reasonableness check is a data validation edit control that matches input data to an occurrence rate.

Licensed to Berend Post berend.post@it-university.nl

Question 1010

Assessments of critical information systems are based on a cyclical audit plan that has not been updated for several years. Which of the following should the IS auditor recommend to BEST address this situation?

- ☐ Use a revolving set of audit plans to cover all systems
- ☐ Update the audit plan quarterly to account for delays and deferrals of periodic reviews
- ☒ Regularly validate the audit plan against business risks
- ☐ Do not include periodic reviews in detail as part of the audit plan

Question 1011

Management has agreed to perform multiple remediation actions in response to an audit issue, including the implementation of a new control. Which of the following is the BEST time for an IS auditor to perform an audit follow-up of this issue?

- ☒ After management has completed the required actions
- ☐ When audit resources are available
- ☐ When management resources are available
- ☐ After the new control has been in place for one year

Question 1012

An IS auditor reviewing a proposed application software acquisition should ensure that the:

- ☐ operating system (OS) being used is compatible with the existing hardware platform.
- ☐ planned OS updates have been scheduled to minimize negative impacts on company needs.
- ☐ OS has the latest versions and updates.
- ☒ products are compatible with the current or planned OS.

Explanation:

Explanation:

Choices A, B and C are incorrect because none of them are related to the area being audited. In reviewing the proposed application, the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice, A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

Licensed to Berend Post berend.post@it-university.nl

Question 1013

Which of the following step of PDCA implement the plan, execute the process and make product?

- ☐ Plan
- ☒ Do
- ☐ Check
- ☐ Act

Explanation:

Do - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition."

The steps in each successive PDCA cycle are:

PLAN

Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

Licensed to Berend Post berend.post@it-university.nl

DO

Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

CHECK

Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

ACT

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

CHECK - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences

ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

Licensed to Berend Post berend.post@it-university.nl

Question 1014

Which of the following is not a common method of multiplexing data?

- ☒ Analytical multiplexing
- ☐ Time-division multiplexing
- ☐ Asynchronous time-division multiplexing
- ☐ Frequency division multiplexing

Explanation:

Generally, the methods for multiplexing data include the following:

Time-division multiplexing (TDM): information from each data channel is allocated bandwidth based on pre-assigned time slots, regardless of whether there is data to transmit.

Asynchronous time-division multiplexing (ATDM): information from data channels is allocated bandwidth as needed, via dynamically assigned time slots.

Frequency division multiplexing (FDM): information from each data channel is allocated bandwidth based on the signal frequency of the traffic.

Statistical multiplexing: Bandwidth is dynamically allocated to any data channels that have information to transmit.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

Question 1015

Which of the following is the BEST detective control for a job scheduling process involving data transmission?

- ☐ Metrics denoting the volume of monthly job failures are reported and reviewed by senior management.
- ☒ Job failure alerts are automatically generated and routed to support personnel.
- ☐ Jobs are scheduled and a log of this activity is retained for subsequent review.
- ☐ Jobs are scheduled to be completed daily and data is transmitted using a secure File Transfer Protocol (FTP).

Question 1016

The PRIMARY reason for an IS auditor to use data analytics techniques is to reduce which type of audit risk?

- ☐ Technology risk
- ☐ Inherent risk
- ☒ Detection risk
- ☐ Control risk

Licensed to Berend Post berend.post@it-university.nl

Question 1017

Which of the following could be determined by an entity-relationship diagram?

- ☒ Links between data objects
- ☐ How the system behaves as a consequence of external events
- ☐ How data are transformed as they move through the system
- ☐ Modes of behavior of data objects

Question 1018

In the event of a disruption or disaster, which of the following technologies provides for continuous operations?

- ☐ Load balancing
- ☒ Fault-tolerant hardware
- ☐ Distributed backups
- ☐ High-availability computing

Explanation:

Explanation:

Fault-tolerant hardware is the only technology that currently supports continuous, uninterrupted service. Load balancing is used to improve the performance of the server by splitting the work between several servers based on workloads. High-availability (HA) computing facilities provide a quick but not continuous recovery, while distributed backups require longer recovery times.

Question 1019

In computer forensics, which of the following is the process that allows bit-for-bit copy of a data to avoid damage of original data or information when multiple analysis may be performed?

- ☒ Imaging
- ☐ Extraction
- ☐ Data Protection
- ☐ Data Acquisition

Explanation:

Imaging is the process that allows one to obtain a bit-for bit copy of a data to avoid damage to the original data or information when multiple analysis may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Licensed to Berend Post berend.post@it-university.nl

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.

Be able to withstand a barrage of legal security

Be unambiguous and not open to misinterpretation.

Licensed to Berend Post berend.post@it-university.nl

Be easily referenced

Contains all information required to explain conclusions reached

Offer valid conclusions, opinions or recommendations when needed

Be created in timely manner.

The following were incorrect answers:

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number367 and 368

Question 1020

Which of the following is MOST important to include in forensic data collection and preservation procedures?

- ☐ Maintaining chain of custody
- ☒ Preserving data integrity
- ☐ Determining tools to be used
- ☐ Assuring the physical security of devices

Licensed to Berend Post berend.post@it-university.nl

Question 1021

Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?

- ☐ Industry standards
- ☐ Information security policy
- ☐ Incident response plan
- ☒ Industry regulations

Question 1022

Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

- ☐ Project database
- ☐ Policy documents
- ☒ Project portfolio database
- ☐ Program organization

Explanation:

Explanation:

A project portfolio database is the basis for project portfolio management. It includes project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. A project database may contain the above for one specific project and updates to various parameters pertaining to the current status of that single project. Policy documents on project management set direction for the design, development, implementation and monitoring of the project. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objective of the project.

Question 1023

Which of the following responsibilities of an organization's quality assurance function should raise concern for an IS auditor?

- ☐ Ensuring the test work supports observations
- ☐ Ensuring standards are adhered to within the development process
- ☒ Implementing solutions to correct defects
- ☐ Updating development methodology

Licensed to Berend Post berend.post@it-university.nl

Question 1024

Which of the following is the MOST effective way to reduce risk to an organization from widespread use of web-based communication technologies?

- ☐ Publish an enterprise-wide policy outlining acceptance use of web-based communication technologies.
- ☒ Incorporate risk awareness training for web-based communications into the IT security program.
- ☐ Monitor staff usage of web-based communication and notify the IT security department of violations.
- ☐ Block access from user devices to unauthorized pages that allow web-based communication.

Question 1025

Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

- ☐ Invite client participation.
- ☐ involve all technical staff.
- ☒ Rotate recovery managers.
- ☐ install locally-stored backup.

Explanation:

Explanation:

Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

Question 1026

Which of the following INCORRECTLY describes the layer function of the Application Layer within the TCP/IP model?

- ☐ Provides user interface
- ☐ Perform data processing such as encryption, encoding, etc
- ☒ Provides reliable delivery
- ☐ Keeps separate the data of different applications

Explanation:

The word INCORRECTLY keyword is used in the question.

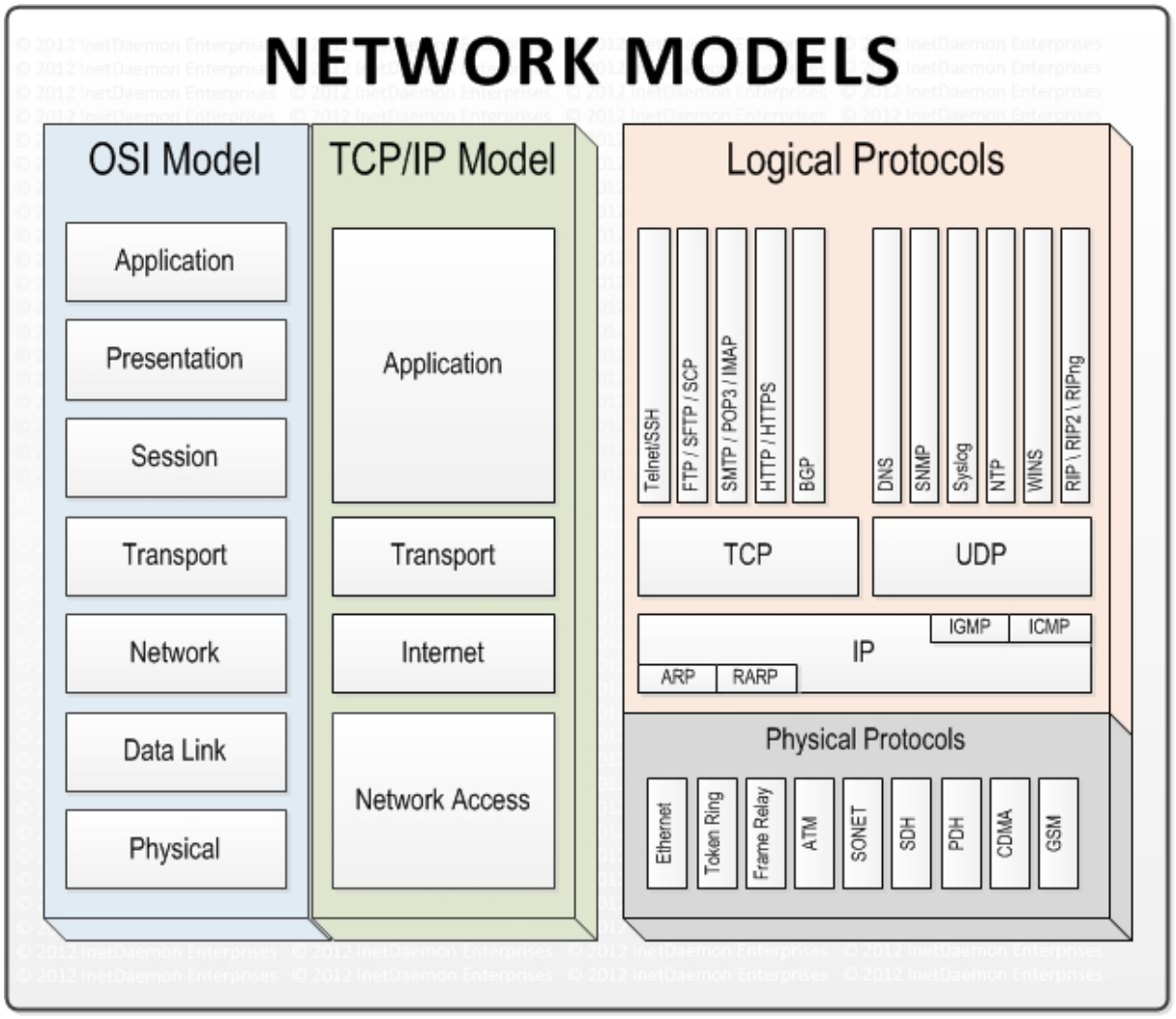
You need to find out the service or functionality which is not performed by application layer of a TCP/IP model.

Licensed to Berend Post berend.post@it-university.nl

The reliable or unreliable delivery of a message is the functionality of transport layer of a TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network Models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Licensed to Berend Post berend.post@it-university.nl

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

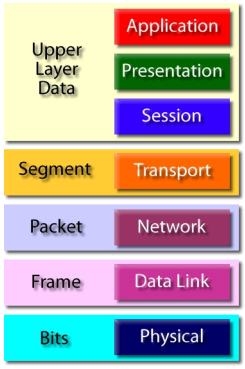
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

Licensed to Berend Post berend.post@it-university.nl

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other options correctly describe functionalities of application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 1027

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- ☐ enhanced reputation.
- ☐ enhanced staff morale.
- ☐ the use of new technology.
- ☒ increased market penetration.

Explanation:

Explanation:

A comprehensive business case for any proposed IT-related business investment should have clearly defined business benefits to enable the expected return to be calculated. These benefits usually fall into two categories: direct and indirect, or soft. Direct benefits usually comprise the quantifiable

Licensed to Berend Post berend.post@it-university.nl

financial benefits that the new system is expected to generate. The potential benefits of enhanced reputation and enhanced staff morale are difficult to quantify, but should be quantified to the extent possible. IT investments should not be made just for the sake of new technology but should be based on a quantifiable business need.

Question 1028

Which of the following correctly describe the potential problem of deploying Wi-Fi Protected Access to secure your wireless network?

- ☐ potential compatibility problems with wireless network interface cards.
- ☒ potential compatibility problems with wireless access points.
- ☐ potential performance problems with wireless network interface cards.
- ☐ potential performance problems with wireless access points.
- ☐ None of the choices.

Explanation:

Explanation:

Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but not necessarily with first generation wireless access points).

Question 1029

Which of the following is the GREATEST risk when relying on reports generated by end-user computing?

- ☒ Data may be inaccurate
- ☐ Reports may not work efficiently
- ☐ Reports may not be timely
- ☐ Historical data may not be available

Question 1030

An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

- ☐ acknowledge receipt of electronic orders with a confirmation message.
- ☐ perform reasonableness checks on quantities ordered before filling orders.
- ☒ verify the identity of senders and determine if orders correspond to contract terms.
- ☐ encrypt electronic orders.

Explanation:

Explanation:

An electronic data interchange (EDI) system is subject not only to the usual risk exposures of computer systems but also to those arising from the potential ineffectiveness of controls on the part of the trading partner and the third-party service provider, making authentication of users and

Licensed to Berend Post berend.post@it-university.nl

messages a major security concern. Acknowledging the receipt of electronic orders with a confirming message is good practice but will not authenticate orders from customers. Performing reasonableness checks on quantities ordered before placing orders is a control for ensuring the correctness of the company's orders, not the authenticity of its customers' orders. Encrypting sensitive messages is an appropriate step but does not apply to messages received.

Question 1031

During Involuntary termination of an employee, which of the following is the MOST important step to be considered?

- ☐ Get a written NDA agreement from an employee
- ☒ Terminate all physical and logical access
- ☐ Provide compensation in lieu of notice period
- ☐ Do not communicate to the respective employee about the termination

Explanation:

For CISA exam you should know below information about Terminated Employee Access

Termination of employment can occur in the following circumstances:

On the request of the employee (Voluntary resignation from service)

Scheduled (On retirement or completion of contract)

Involuntary (forced by management in special circumstances)

In case of an involuntary termination of employment, the logical and physical access rights of employees to the IT infrastructure should either be withdrawn completely or highly restricted as early as possible, before the employee become aware of termination or its likelihood.

This ensures that terminated employees cannot continue to access potentially confidential or damaging information from the IT resources or perform any action that would result in damage of any kind of IT infrastructure, applications and data. Similar procedure in place to terminate access for third parties upon terminating their activities with the organization.

When it is necessary for employee to continue to have accesses, such access must be monitored carefully and continuously and should take place with senior management's knowledge and authorization.

In case of a voluntary or scheduled termination of employment, it is management's prerogative to decide whether access is restricted or withdrawn. This depends on:

Licensed to Berend Post berend.post@it-university.nl

The specific circumstances associated with each case

The sensitivity of employee's access to the IT infrastructure and resources

The requirement of the organization's information security policies, standards and procedure.

The following were incorrect answers:

The other options presented are incorrectly describes about involuntary termination.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 361 and 362

Question 1032

An IS auditor is unable to directly test privacy controls for a client's cloud-based application. The MOST effective alternative to direct testing is to review:

- ☐ the provider's internal audit reports.
- ☐ the provider's statement of assurance.
- ☐ formal privacy certification.
- ☒ independent audit reports.

Question 1033

Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords, etc?

- ☐ Smurf attack
- ☐ Traffic analysis
- ☒ Harming
- ☐ Interrupt attack

Explanation:

Harming is a cyber attack intended to redirect a website's traffic to another, bogus site. Harming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Harming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

The term "phrasing" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both phrasing and phishing have been used to gain information for online identity theft. Phrasing has become of major concern to businesses hosting ecommerce and online banking

 Licensed to Berend Post berend.post@it-university.nl

websites. Sophisticated measures known as anti-harming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against harming.

For your exam you should know the information below:

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information about their target to increase their probability of success.

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the are tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article entitled "Genuine"; clicking on it will in fact take the user to the article entitled "Deception". In the lower left hand corner of most browsers users can preview and verify where the link is going to take them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery

Once a victim visits the phishing website, the deception is not over. Some phishing scams use JavaScript commands in order to alter the address bar. This is done either by placing a picture of a legitimate URL over the address bar, or by closing the original bar and opening up a new one with the legitimate URL.

 Licensed to Berend Post berend.post@it-university.nl

An attacker can even use flaws in a trusted website's own scripts against the victim. These types of attacks (known as cross-site scripting) are particularly problematic, because they direct the user to sign in at their bank or service's own web page, where everything from the web address to the security certificates appears correct. In reality, the link to the website is crafted to carry out the attack, making it very difficult to spot without specialist knowledge.

The following answers are incorrect:

Smurf Attack – Occurs when mix-configured network device allow packet to be sent to all hosts on a particular network via the broadcast address of the network

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Interrupt attack- Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 323

Official ISC2 guide to CISSP CBK 3rd Edition Page number326

http://en.wikipedia.org/wiki/Phishing

http://en.wikipedia.org/wiki/Pharming

Question 1034

Which of the following is the MOST effective way to ensure security policies are relevant to organizational business practices?

- ☐ Leverage security steering committee contribution.
- ☒ Obtain senior management sign-off.
- ☐ Integrate industry best practices.
- ☐ Conduct an organization-wide security audit.

Licensed to Berend Post berend.post@it-university.nl

Question 1035

Email required for business purposes is being stored on employees' personal devices. Which of the following is an IS auditor's BEST recommendation?

- ☐ Implement an email containerization solution on personal devices
- ☐ Prohibit employees from storing company email on personal devices.
- ☐ Ensure antivirus to utilize passwords on personal devices.
- ☒ Require employees to utilize passwords on personal devices.

Question 1036

Which of the following results in a denial-of-service attack?

- ☐ Brute force attack
- ☒ Ping of death
- ☐ Leapfrog attack
- ☐ Negative acknowledgement (NAK) attack

Explanation:

Explanation:

The use of Ping with a packet size higher than 65 KB and no fragmentation flag on will cause a denial of service. A brute force attack is typically a text attack that exhausts all possible key combinations. A leapfrog attack, the act of tenting through one or more hosts to preclude a trace, makes use of user ID and password information obtained illicitly from one host to compromise another host. A negative acknowledgement attack is a penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, leaving the system in an unprotected state during such interrupts.

Question 1037

To ensure message integrity, confidentiality and non-repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

- ☒ the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.
- ☐ any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key.
- ☐ the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering both the encrypted message and digest using the receiver's public key.
- ☐ the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Applying a cryptographic hashing algorithm against the entire message addresses the message integrity issue. Enciphering the message digest using the sender's private key addresses non repudiation. Encrypting the message with a symmetric key, thereafter allowing the key to be enciphered using the receiver's public key, most efficiently addresses the confidentiality of the message as well as the receiver's non repudiation. The other choices would address only a portion of the requirements.

Question 1038

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

- ☐ increase the time allocated for system testing
- ☒ implement formal software inspections
- ☐ increase the development staff
- ☐ Require the sign-off of all project deliverables

Explanation:

Explanation: inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce.

Deliverable reviews normally do not go down to the same level of detail as software inspections.

Question 1039

Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

- ☒ The organization does not have control over encryption.
- ☐ Messages are subjected to wiretapping.
- ☐ Data might not reach the intended recipient.
- ☐ The communication may not be secure.

Explanation:

Explanation:

The SSL security protocol provides data encryption, server authentication, message integrity and optional client authentication. Because SSL is built into all major browsers and web servers, simply installing a digital certificate turns on the SSL capabilities. SSL encrypts the datum while it is being

Licensed to Berend Post berend.post@it-university.nl

transmitted over the internet. The encryption is done in the background, without any interaction from the user; consequently, there is no password to remember. The other choices are incorrect. Since the communication between client and server is encrypted, the confidentiality of information is not affected by wiretapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted data. All data sent over an encrypted SSL connection are protected with a mechanism to detect tampering, i.e., automatically determining whether data has been altered in transit.

Question 1040

Which of the following step of PDCA study the actual result and compares it against the expected result?

- ☐ Plan
- ☐ Do
- ☒ Check
- ☐ Act

Explanation:

Check - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition."

The steps in each successive PDCA cycle are:

Licensed to Berend Post berend.post@it-university.nl

PLAN

Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

DO

Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

CHECK

Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

ACT

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

Licensed to Berend Post berend.post@it-university.nl

DO - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

Question 1041

An internal audit department recently established a quality assurance (QA) program. Which of the following activities is MOST important to include as part of the QA program requirements?

- ☒ Ongoing monitoring of the audit activities
- ☐ Analysis of user satisfaction reports from business lines.
- ☐ Feedback from internal audit staff
- ☐ Long-term internal audit resource planning

Question 1042

What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

- ☐ A first-generation packet-filtering firewall
- ☐ A circuit-level gateway
- ☒ An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
- ☐ An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Explanation:

Explanation:

An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

Licensed to Berend Post berend.post@it-university.nl

Question 1043

Which of the following cloud deployment model is formed by the composition of two or more cloud deployment mode?

- ☐ Private Cloud
- ☐ Community Cloud
- ☐ Public Cloud
- ☒ Hybrid Cloud

Explanation:

In Hybrid cloud, the cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

For your exam you should know below information about Cloud Computing deployment models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Private Cloud

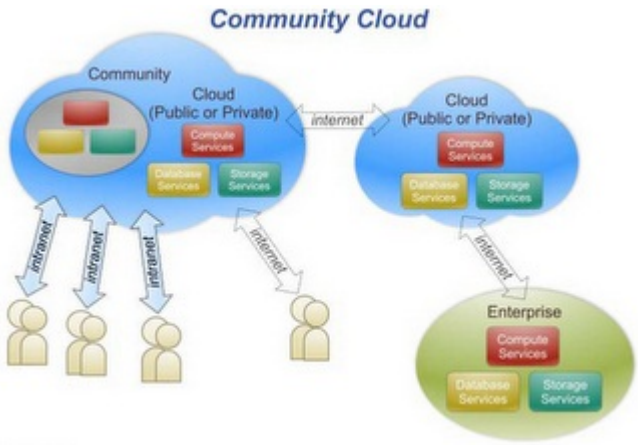
Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance

Licensed to Berend Post berend.post@it-university.nl

considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

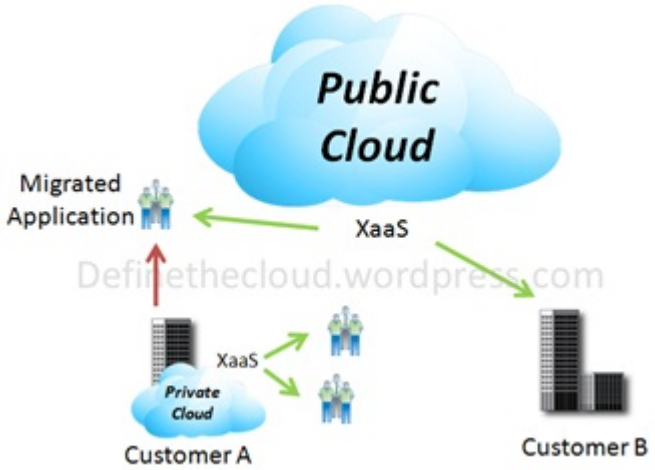
Community Cloud



Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Public Cloud

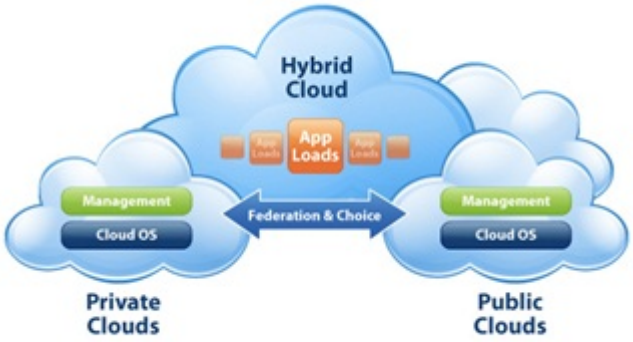


Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Licensed to Berend Post berend.post@it-university.nl

hybrid cloud



The following answers are incorrect:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

Licensed to Berend Post berend.post@it-university.nl

Question 1044

You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):

- ☒ 60 - 75 degrees Fahrenheit
- ☒ 10 - 25 degrees Celsius
- ☐ 30 - 45 degrees Fahrenheit
- ☐ 1 - 15 degrees Celsius
- ☐ 20 - 35 degrees Fahrenheit
- ☐ 0 - 5 degrees Celsius

Explanation:

Explanation:

You should keep all computer rooms at reasonable temperatures, which is in between 60 - 75 degrees Fahrenheit or 10 - 25 degrees Celsius. You should also keep humidity levels at 20 - 70 percent.

Question 1045

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

- ☐ Blowfish
- ☐ Tripwire
- ☐ certificate
- ☐ DES
- ☒ one-time pad
- ☐ None of the choices.

Explanation:

Explanation:

It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

Licensed to Berend Post berend.post@it-university.nl

Question 1046

A vulnerability in which of the following virtual systems would be of GREATEST concern to the IS auditor?

- ☒ The virtual machine management server
- ☐ The virtual file server
- ☐ The virtual application server
- ☐ The virtual antivirus server

Question 1047

A core tenant of an IS strategy is that it must:

- ☐ Be inexpensive
- ☐ Be protected as sensitive confidential information
- ☐ Protect information confidentiality, integrity, and availability
- ☒ Support the business objectives of the organization

Explanation:

Explanation:

Above all else, an IS strategy must support the business objectives of the organization.

Question 1048

Which of the following level in CMMI model focuses on process innovation and continuous optimization?

- ☐ Level 4
- ☒ Level 5
- ☐ Level 3
- ☐ Level 2

Explanation:

Level 5 is the optimizing process and focus on process innovation and continuous integration.

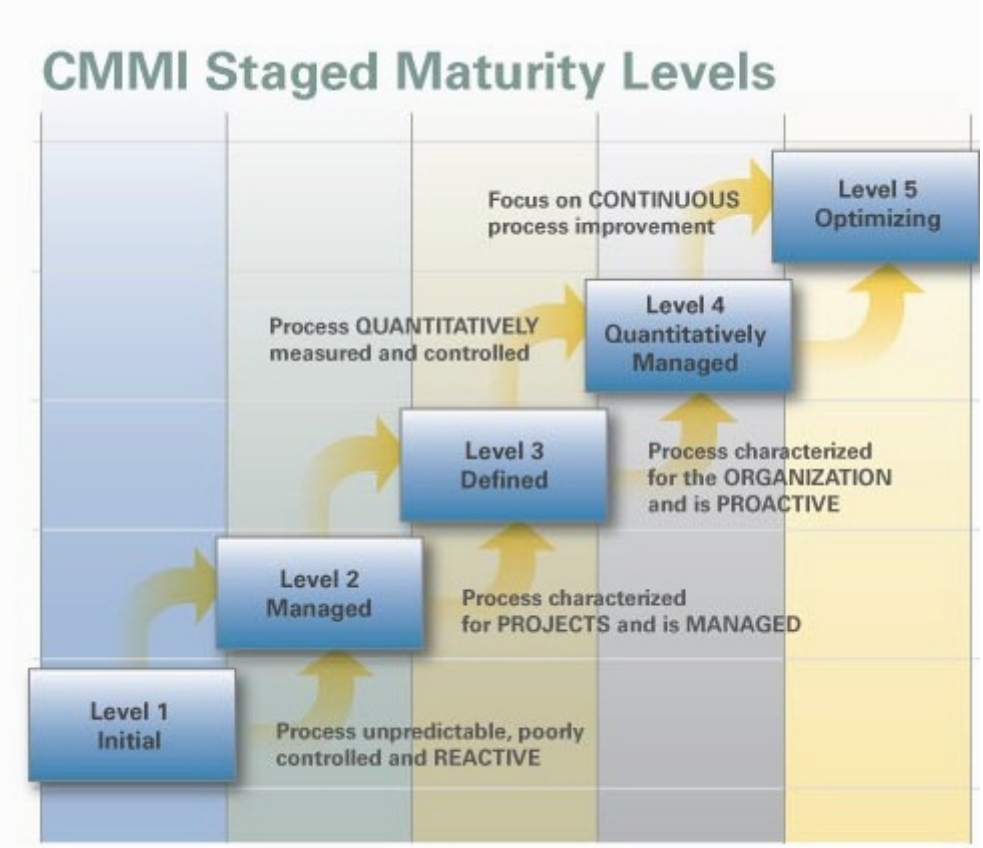
For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.

CMMI Levels

Licensed to Berend Post berend.post@it-university.nl



A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organizations' software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

Licensed to Berend Post berend.post@it-university.nl

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".[citation needed]

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.

Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions).

Managed - the process is quantitatively managed in accordance with agreed-upon metrics.

Optimizing - process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Licensed to Berend Post berend.post@it-university.nl

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

The following were incorrect answers:

Level 4 – Focus on process management and process control

Level 3 – Process definition and process deployment.

Level 2 – Performance management and work product management.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Licensed to Berend Post berend.post@it-university.nl

Question 1049

An IS auditor is involved in the user testing phase of a development project. The developers wish to use a copy of a peak volume transaction file from the production process to show that the development can cope with the required volume. What is the auditor's PRIMARY concern?

- ☒ Sensitive production data may be read by unauthorized persons.
- ☐ The error-handling and credibility checks may not be fully proven.
- ☐ Users may not wish for production data to be made available for testing.
- ☐ All functionality of the new process may not be tested.

Question 1050

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key.
True or false?

- ☐ False
- ☒ True

Explanation:

Explanation:

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the sender's public key.

Question 1051

After reviewing its business processes, a large organization is deploying a new web application based on a VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

- ☐ Fine-grained access control
- ☒ Role-based access control (RBAC)
- ☐ Access control lists
- ☐ Network/service access control

Explanation:

Explanation:

Authorization in this VoIP case can best be addressed by role-based access control (RBAC) technology. RBAC is easy to manage and can enforce strong and efficient access controls in large-scale web environments including VoIP implementation. Access control lists and fine- grained access control on VoIP web applications do not scale to enterprise wide systems, because they are primarily based on individual user identities and their specific technical privileges. Network/service addresses VoIP availability but does not address application-level access or authorization.

Licensed to Berend Post berend.post@it-university.nl

Question 1052

Which of the following is the BEST reason to certify an organization to an international security standard?

- ☐ The certification covers enterprise security end-to-end.
- ☐ The certification reduces information security risk.
- ☐ The certification ensures that optimal controls are in place.
- ☒ The certification delivers value to stakeholders.

Question 1053

Which of the following should be the FIRST step when drafting an incident response plan for a new cyber-attack scenario?

- ☐ Schedule response testing
- ☐ Create a new incident response team
- ☐ Create a reporting template
- ☒ Identify relevant stakeholders

Question 1054

Talking about biometric measurement, which of the following measures the percent of invalid users who are incorrectly accepted in?

- ☐ failure to reject rate
- ☒ false accept rate
- ☐ false reject rate
- ☐ failure to enroll rate
- ☐ None of the choices.

Explanation:

Explanation:

Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted in, while the FRR measures the percent of valid users who are wrongly rejected.

Licensed to Berend Post berend.post@it-university.nl

Question 1055

During a help desk review, an IS auditor determines the call abandonment rate exceeds agreed-upon service levels. What conclusions can be drawn from this finding?

- ☐ There are insufficient telephone lines available to the help desk.
- ☒ There is insufficient staff to handle the help desk call volume.
- ☐ Help desk staff are unable to resolve a sufficient number of problems on the first call.
- ☐ Users are finding solutions from alternative sources.

Question 1056

Which of the following is the MOST important factor when determining the frequency of information security risk reassessment?

- ☐ Audit findings
- ☐ Risk priority
- ☐ Mitigating controls
- ☒ Risk metrics

Question 1057

Which of the following occurs during the issues management process for a system development project?

- ☐ Contingency planning
- ☐ Impact assessment
- ☐ Configuration management
- ☒ Help desk management

Question 1058

An IS auditor has completed a service level management audit related to order management services provided by a third party. Which of the following is the MOST significant finding?

- ☐ The third party has offshore support arrangements.
- ☒ Penalties for missing service levels are limited.
- ☐ The service level agreement does not define how availability is measured.
- ☐ Service desk support is not available outside the company's business hours.

Licensed to Berend Post berend.post@it-university.nl

Question 1059

To minimize the cost of a software project, quality management techniques should be applied:

- ☐ as close to their writing (i.e., point of origination) as possible.
- ☐ primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
- ☒ continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
- ☐ mainly at project close-down to capture lessons learned that can be applied to future projects.

Explanation:

Explanation:

While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

Question 1060

An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

Licensed to Berend Post berend.post@it-university.nl

Question 1061

Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack?

- ☐ Inbound traffic filtering
- ☐ Using access control lists (ACLs) to restrict inbound connection attempts
- ☒ Outbound traffic filtering
- ☐ Recentralizing distributed systems

Explanation:

Explanation:

Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

Question 1062

To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☐ The business objectives of the organization
- ☐ The effect of segregation of duties on internal controls
- ☒ The point at which controls are exercised as data flows through the system
- ☐ Organizational control policies

Explanation:

Explanation:

When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

Question 1063

An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

- ☐ Obtain senior management sponsorship.
- ☐ Identify business needs.
- ☒ Conduct a paper test.
- ☐ Perform a system restore test.

Explanation:

Explanation:

A best practice would be to conduct a paper test. Senior management sponsorship and business needs identification should have been obtained prior to implementing the plan. A paper test should be conducted first, followed by system or full testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1064

Which of the following is the BEST method for uncovering shadow IT within an organization?

- ☐ Analyze help desk tickets.
- ☐ Review secondary approval thresholds.
- ☒ Use a cloud access security broker (CASB).
- ☐ Review business processes.

Question 1065

Which of the following layer of an OSI model transmits and receives the bit stream as electrical, optical or radio signals over an appropriate medium or carrier?

- ☐ Transport Layer
- ☐ Network Layer
- ☐ Data Link Layer
- ☒ Physical Layer

Explanation:

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

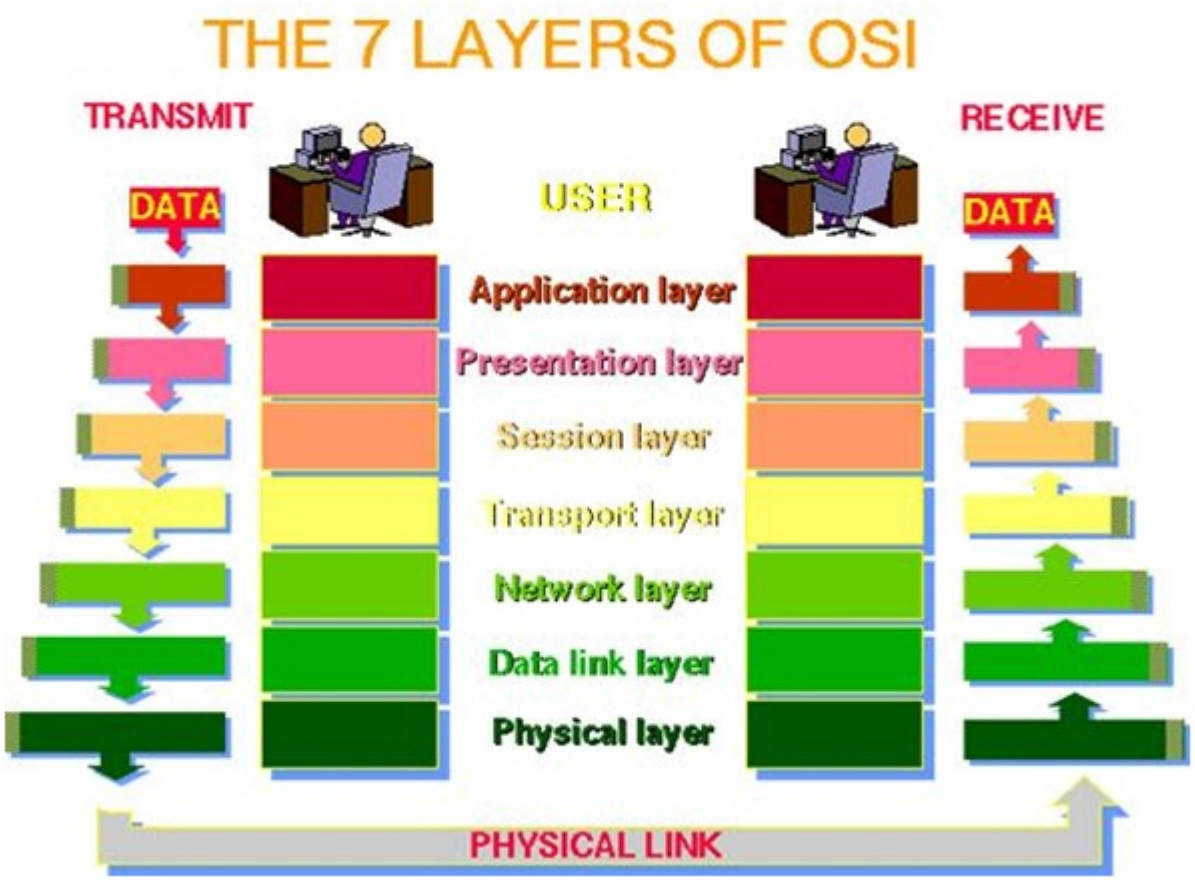
For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model

Licensed to Berend Post berend.post@it-university.nl



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Licensed to Berend Post berend.post@it-university.nl

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

Licensed to Berend Post berend.post@it-university.nl

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

Licensed to Berend Post berend.post@it-university.nl

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.

Data link layer - The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Question 1066

The ability of the internal IS audit function to achieve desired objectives depends largely on:

- ☐ the training of audit personnel
- ☐ the background of audit personnel
- ☒ the independence of audit personnel
- ☐ the performance of audit personnel
- ☐ None of the choices.

Explanation:

Explanation:

The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Top management should ensure that the audit department does not participate in activities that may compromise its independence.

Question 1067

Which of the following would be of GREATEST concern to an IS auditor receiving an organization's security incident handling procedures?

- ☐ Annual tabletop exercises are performed instead of functional incident response exercises.
- ☐ Roles for computer emergency response team (CERT) members have not been formally documented.
- ☐ Guidelines for prioritizing incidents have not been identified.
- ☒ Workstation antivirus software alerts are not regularly reviewed.

Licensed to Berend Post berend.post@it-university.nl

Question 1068

In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?

- ☐ Update the corporate mobile usage policy to prohibit texting.
- ☐ Conduct a business impact analysis (BIA) and provide the report to management.
- ☐ Stop providing mobile devices until the organization is able to implement controls.
- ☒ Include the topic of prohibited texting in security awareness training.

Question 1069

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

- ☒ Session keys are dynamic
- ☐ Private symmetric keys are used
- ☐ Keys are static and shared
- ☐ Source addresses are not encrypted or authenticated

Explanation:

Explanation:

WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy (WEP), which operates with static keys (same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

Question 1070

In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

- ☒ Foreign key
- ☐ Primary key
- ☐ Secondary key
- ☐ Public key

Explanation:

Explanation:

In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database. It should not be possible to delete a row from a customer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table, so it is not able to provide/ensure referential integrity by itself. Secondary keys that are not foreign keys are not subject to referential integrity checks. Public key is related to encryption and not linked in any way to referential integrity.

Licensed to Berend Post berend.post@it-university.nl

Question 1071

Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

- ☐ Logic bombs
- ☐ Phishing
- ☐ Spyware
- ☒ Trojan horses

Explanation:

Explanation:

Trojan horses are malicious or damaging code hidden within an authorized computer program. Hackers use Trojans to mastermind DDOS attacks that affect computers that access the same Internet site at the same moment, resulting in overloaded site servers that may no longer be able to process legitimate requests. Logic bombs are programs designed to destroy or modify data at a specific time in the future. Phishing is an attack, normally via e-mail, pretending to be an authorized person or organization requesting information. Spyware is a program that picks up information from PC drives by making copies of their contents.

Question 1072

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

- ☐ eavesdropping
- ☐ spoofing.
- ☒ traffic analysis.
- ☐ masquerading.

Explanation:

Explanation:

In traffic analysis, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, and the intruder is able to guess the type of communication taking place. This typically is used when messages are encrypted and eavesdropping would not yield any meaningful results, in eavesdropping, which also is a passive attack, the intruder gathers the information flowing through the network with the intent of acquiring and releasing message contents for personal analysis or for third parties. Spoofing and masquerading are active attacks, in spoofing, a user receives an e-mail that appears to have originated from one source when it actually was sent from another source. In masquerading, the intruder presents an identity other than the original identity.

Licensed to Berend Post berend.post@it-university.nl

Question 1073

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- ☐ Check digit
- ☐ Existence check
- ☒ Completeness check
- ☐ Reasonableness check

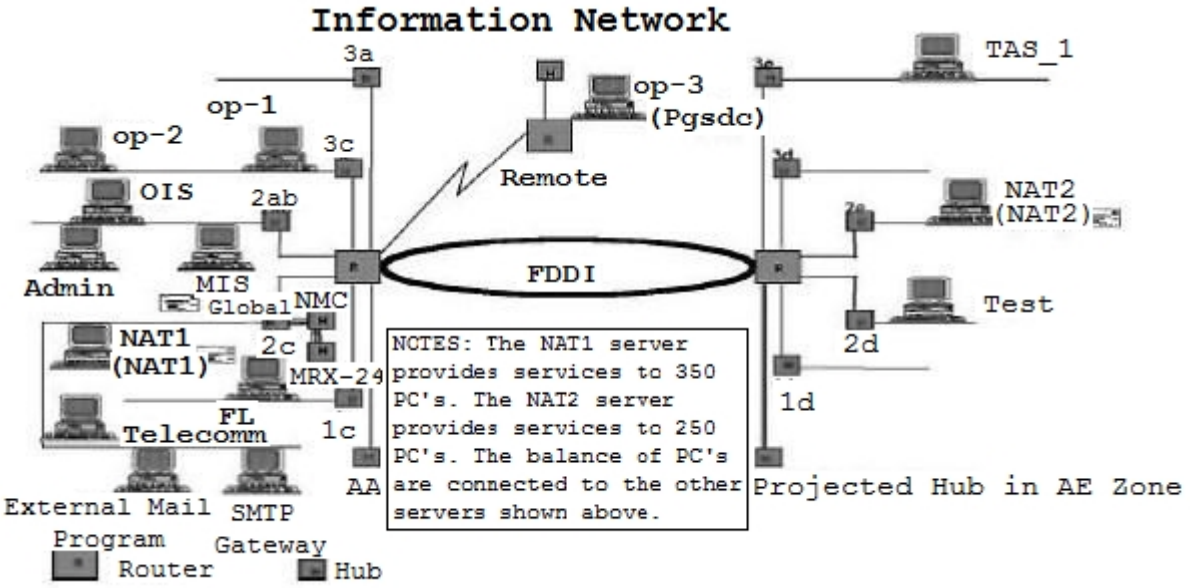
Explanation:

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks.

Question 1074

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



- ☐ Virus attack
- ☒ Performance degradation
- ☐ Poor management controls
- ☐ Vulnerability to external hackers

Explanation:

Explanation:

Hubs are internal devices that usually have no direct external connectivity, and thus are not prone to hackers. There are no known viruses that are specific to hub attacks. While this situation may be an indicator of poor management controls, choice B is more likely when the practice of stacking hubs and creating more terminal connections is used.

Licensed to Berend Post berend.post@it-university.nl

Question 1075

Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs (choose the most precise answer)?

- ☒ rootkits
- ☐ virus
- ☐ trojan
- ☐ tripwire
- ☐ None of the choices.

Explanation:

Explanation:

"A backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing ""legitimate"" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports."

Question 1076

What is wrong with a Black Box type of intrusion detection system?

- ☐ you cannot patch it
- ☐ you cannot test it
- ☒ you cannot examine its internal workings from outside.
- ☐ you cannot tune it
- ☐ None of the choices.

Explanation:

Explanation:

"An intrusion detection system should be able to run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a "black box", because you want to ensure its internal workings are examinable from outside."

Question 1077

Two-factor authentication can be circumvented through which of the following attacks?

- ☐ Denial-of-service
- ☒ Man-in-the-middle
- ☐ Key logging
- ☐ Brute force

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A man-in-the-middle attack is similar to piggybacking, in that the attacker pretends to be the legitimate destination, and then merely retransmits whatever is sent by the authorized user along with additional transactions after authentication has been accepted. A denial-of- service attack does not have a relationship to authentication. Key logging and brute force could circumvent a normal authentication but not a two-factor authentication.

Question 1078

Which of the following internet security threats could compromise integrity?

- ☐ Theft of data from the client
- ☐ Exposure of network configuration information
- ☒ A Trojan horse browser
- ☐ Eavesdropping on the net

Explanation:

Explanation:

Internet security threats/vulnerabilities to integrity include a Trojan horse, which could modify user data, memory and messages found in client-browser software. The other options compromise confidentiality.

Question 1079

Which of the following statement INCORRECTLY describes network device such as a Router?

- ☐ Router creates a new header for each packet
- ☒ Router builds a routing table based on MAC address
- ☐ Router does not forward broadcast packet
- ☐ Router assigns a different network address per port

Explanation:

The INCORRECTLY keyword is used in the question. You need to find out a statement which is not valid about router. Router builds a routing table based on IP address and not on MAC address.

Difference between Router and Bridge:

Router

Bridge

Creates a new header for each packet

Does not alter header. Only reads the header

Builds routing table based on IP address

 Licensed to Berend Post berend.post@it-university.nl

Build forwarding table based on MAC address

Assigns a different network address per port

Use the same network address for all ports

Filters traffic based on IP address

Filter traffic based on MAC address

Does not forward broadcast packet

Forward broadcast packet

Does not forward traffic that contain destination address unknown to the router

Forward traffic if destination address is unknown to bridge

For your exam you should know below information about network devices:

Repeaters

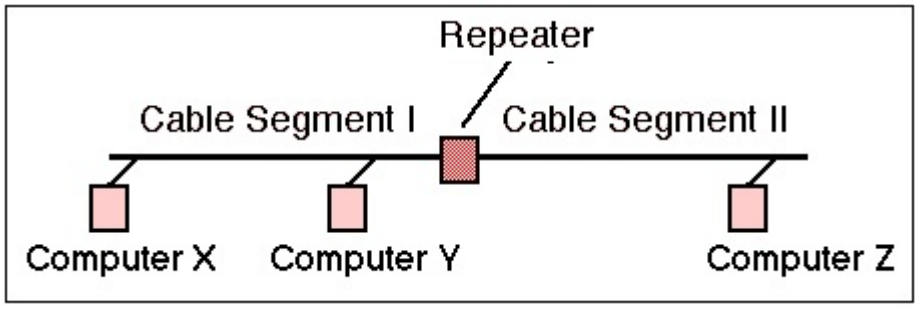
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.

A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Licensed to Berend Post berend.post@it-university.nl

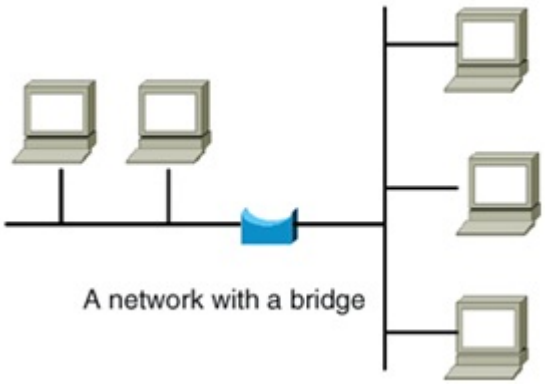
Repeater



Bridges

A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge



Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Licensed to Berend Post berend.post@it-university.nl

Router and Switch

Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

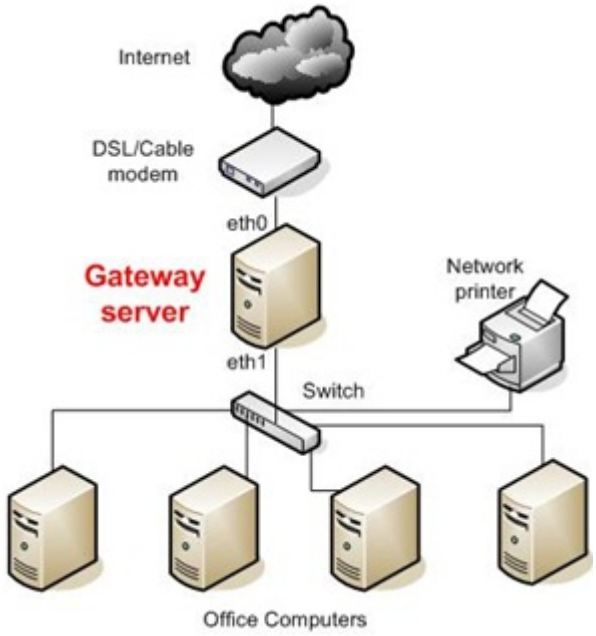
Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions.

Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

Licensed to Berend Post berend.post@it-university.nl



The following were incorrect answers:

The other options presented correctly describes about Router.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 263

Question 1080

With the help of a security officer, granting access to data is the responsibility of:

- ☒ data owners.
- ☐ programmers.
- ☐ system analysts.
- ☐ librarians.

Explanation:

Explanation:

Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners' approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

Licensed to Berend Post berend.post@it-university.nl

Question 1081

Which of the following is widely accepted as one of the critical components in networking management?

- ☒ Configuration management
- ☐ Topological mappings
- ☐ Application of monitoring tools
- ☐ Proxy server troubleshooting

Explanation:

Explanation:

Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally, it also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server troubleshooting is used for troubleshooting purposes.

Question 1082

During a review of an organization's IT incident management practices, the IS auditor finds the quality of incident resolution documentation is poor. Which of the following is the BEST recommendation to help address this issue?

- ☐ Have service desk staff create documentation be choosing from pre-selected answers in the service management tool.
- ☐ Require service desk staff to open incident tickets only when they have sufficient information.
- ☒ Revise incident resolution procedures and provide training for service desk staff on the applicable updates.
- ☐ Require peer review of resolution documentation followed by service desk management sign off.

Question 1083

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- ☐ the existing IT environment.
- ☒ the business plan.
- ☐ the present IT budget.
- ☐ current technology trends.

Explanation:

Explanation:

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

Licensed to Berend Post berend.post@it-university.nl

Question 1084

An organization uses electronic funds transfer (EFT) to pay its vendors. Which of the following should be an IS auditor's MAIN focus while reviewing controls in the accounts payable application?

- ☒ Changes to the vendor master file
- ☐ Volume of transactions
- ☐ Amount of disbursements
- ☐ Frequency of transactions

Question 1085

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- ☐ The data should be deleted and overwritten with binary 0s.
- ☒ The data should be demagnetized.
- ☐ The data should be low-level formatted.
- ☐ The data should be deleted.

Explanation:

Explanation:

To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

Question 1086

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

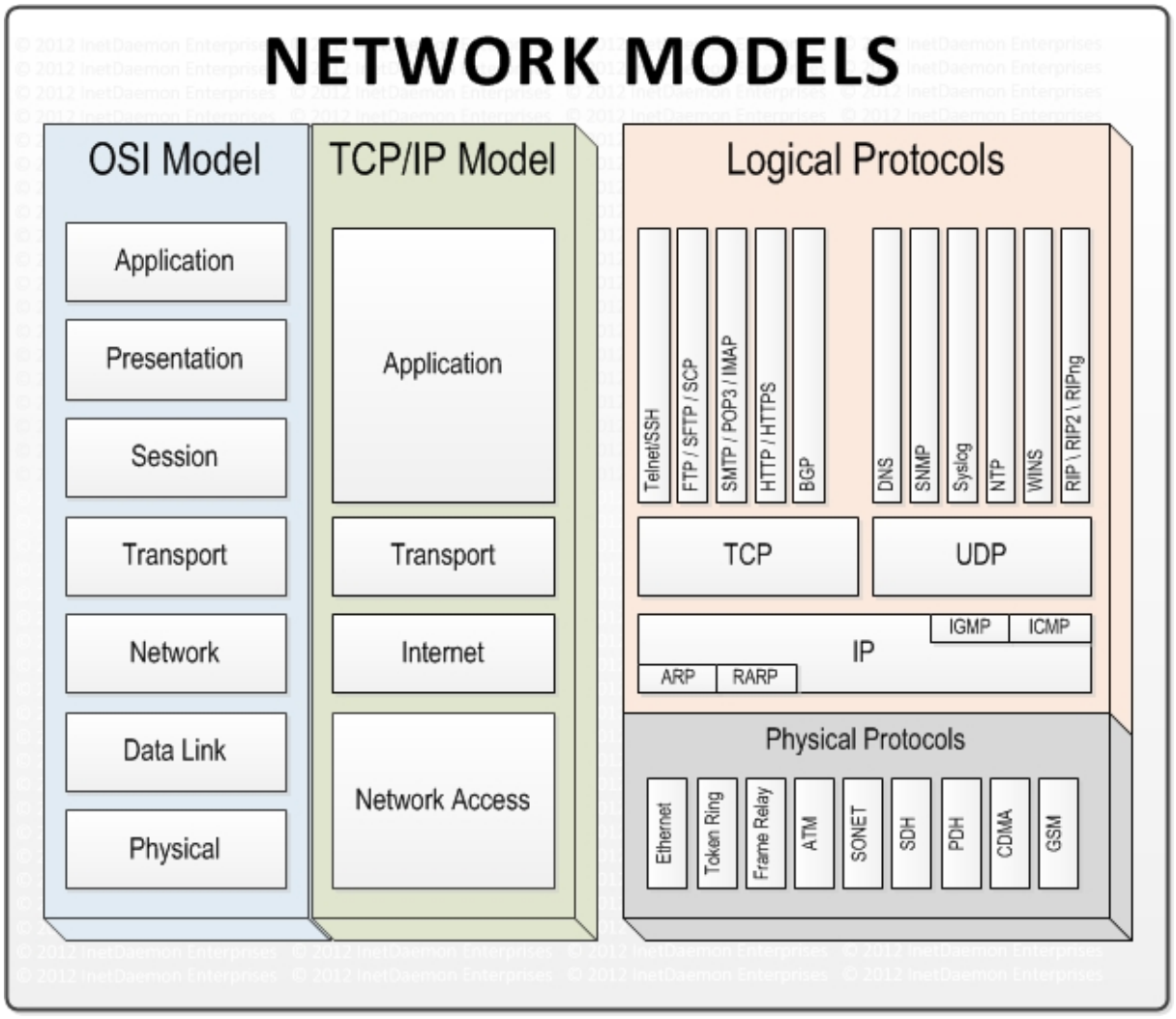
- ☐ Data
- ☒ Segment
- ☐ Packet
- ☐ Frame

Explanation:

For your exam you should know below information about TCP/IP model:

Network models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

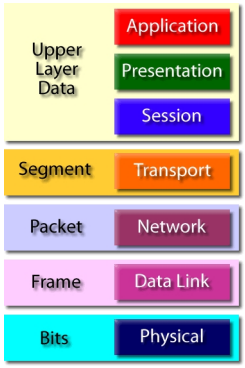
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

Data – Application layer PDU

Packet – Network interface layer PDU

Frame/bit – LAN or WAN interface layer PDU

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 1087

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

- ☐ Full operational test
- ☒ Preparedness test
- ☐ Paper test
- ☐ Regression test

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery. A paper test is a structured walk- through of the disaster recovery plan and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a disaster recovery planning (DRP) test and is used in software maintenance.

Question 1088

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

- ☐ users may prefer to use contrived data for testing.
- ☒ unauthorized access to sensitive data may result.
- ☐ error handling and credibility checks may not be fully proven.
- ☐ the full functionality of the new process may not necessarily be tested.

Explanation:

Explanation:

Unless the data are sanitized, there is a risk of disclosing sensitive data.

Question 1089

Which of the following is the MOST reasonable option for recovering a noncritical system?

- ☐ Warm site
- ☐ Mobile site
- ☐ Hot site
- ☒ Cold site

Explanation:

Explanation:

Generally, a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of operations. A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

Licensed to Berend Post berend.post@it-university.nl

Question 1090

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the CRC- 32 checksum for:

- ☒ integrity.
- ☐ validity.
- ☐ accuracy.
- ☐ confidentiality.
- ☐ None of the choices.

Explanation:

Explanation:

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

Many WEP systems require a key in hexadecimal format. If one chooses keys that spell words in the limited 0-9, A-F hex character set, these keys can be easily guessed.

Question 1091

Sending a message and a message hash encrypted by the sender's private key will ensure:

- ☒ authenticity and integrity.
- ☐ authenticity and privacy.
- ☐ integrity and privacy.
- ☐ privacy and nonrepudiation.

Explanation:

Explanation:

If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender's public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute.

Authenticity and privacy will be ensured by first using the sender's private key and then the receiver's public key to encrypt the message. Privacy and integrity can be ensured by using the receiver's public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender's private key to encrypt the message. The sender's public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

Licensed to Berend Post berend.post@it-university.nl

Question 1092

Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:

- ☐ most privilege
- ☐ full privilege
- ☒ least privilege
- ☐ null privilege
- ☐ None of the choices.

Explanation:

Explanation:

There are two different approaches to security in computing. One focuses mainly on external threats, and generally treats the computer system itself as a trusted system. The other regards the computer system itself as largely an untrusted system, and redesigns it to make it more secure in a number of ways.

This technique enforces the principle of least privilege to great extent, where an entity has only the privileges that are needed for its function.

Question 1093

An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

- ☒ Substantive
- ☐ Compliance
- ☐ Integrated
- ☐ Continuous audit

Explanation:

Explanation:

Using a statistical sample to inventory the tape library is an example of a substantive test.

Question 1094

When introducing a maturity model to the IT management process, it is BEST to align the maturity level to a point that reflects which of the following?

- ☒ Ideal business production level
- ☐ Minimum cost expenditure level
- ☐ Maximum risk tolerance level
- ☐ Industry-standard practice level

Licensed to Berend Post berend.post@it-university.nl

Question 1095

A manufacturing company is implementing application software for its sales and distribution system. Which of the following is the MOST important reason for the company choose a centralized online database?

- ☐ Enhanced data redundancy
- ☒ Elimination of multiple points of failure
- ☐ Elimination of the need for data normalization
- ☐ Enhanced integrity controls

Question 1096

Following significant organizational changes, which of the following is the MOST important consideration when updating the IT policy?

- ☐ The policy is integrated into job descriptions.
- ☐ The policy is endorsed by senior executives.
- ☒ The policy is compliant with relevant laws and regulations.
- ☐ The policy is aligned with industry standards and best practice.

Question 1097

When considering whether to adopt bring your own device (BYOD), it is MOST important for the information security manager to ensure that:

- ☒ security controls are applied to each device when joining the network
- ☐ business leaders have an understanding of security risks
- ☐ users have read and signed acceptable use agreements
- ☐ the applications are tested prior to implementation

Question 1098

In planning a major system development project, function point analysis would assist in:

- ☐ estimating the elapsed time of the project.
- ☐ estimating the size of a system development task.
- ☒ analyzing the functions undertaken by system users as an aid to job redesign.
- ☐ determining the business functions undertaken by a system or program.

Licensed to Berend Post berend.post@it-university.nl

Question 1099

Why is one-time pad not always preferable for encryption (choose all that apply):

- ☒ it is difficult to use securely.
- ☒ it is highly inconvenient to use.
- ☐ it requires licensing fee.
- ☐ it requires internet connectivity.
- ☐ it is Microsoft only.
- ☐ None of the choices.

Explanation:

Explanation:

It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad - has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

Question 1100

Due to a recent business divesture, an organization has limited IT resources to deliver critical projects. Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

- ☐ Peer organizational staffing benchmarks
- ☐ Budgeted forecast for the next financial year
- ☒ Human resources sourcing strategy
- ☐ Records of actual time spent on projects

Question 1101

Which of the following protects against the impact of temporary and rapid decreases or increases in electricity?

- ☐ Redundant power supply
- ☐ Emergency power-off switch
- ☐ Stand-by generator
- ☒ Uninterruptible power supply (UPS)

Licensed to Berend Post berend.post@it-university.nl

Question 1102

The most likely error to occur when implementing a firewall is:

- ☒ incorrectly configuring the access lists.
- ☐ compromising the passwords due to social engineering.
- ☐ connecting a modem to the computers in the network.
- ☐ inadequately protecting the network and server from virus attacks.

Explanation:

Explanation:

An updated and flawless access list is a significant challenge and, therefore, has the greatest chance for errors at the time of the initial installation. Passwords do not apply to firewalls, a modem bypasses a firewall and a virus attack is not an element in implementing a firewall.

Question 1103

E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

- ☒ sender's private key and encrypting the message using the receiver's public key.
- ☐ sender's public key and encrypting the message using the receiver's private key.
- ☐ receiver's private key and encrypting the message using the sender's public key.
- ☐ receiver's public key and encrypting the message using the sender's private key.

Explanation:

Explanation:

By signing the message with the sender's private key, the receiver can verify its authenticity using the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt the message using their own private key. The receiver's private key is confidential and, therefore, unknown to the sender. Messages encrypted using the sender's private key can be read by anyone with the sender's public key.

Question 1104

The BEST access strategy while configuring a firewall would be to:

- ☐ permit access to all and log the activity
- ☐ deny access to all but permit selected
- ☐ permit access to all but deny selected
- ☒ deny access to all except authorized programs

Licensed to Berend Post berend.post@it-university.nl

Question 1105

Which of the following is a data validation edit and control?

- ☐ Hash totals
- ☒ Reasonableness checks
- ☐ Online access controls
- ☐ Before and after image reporting

Explanation:

Explanation:

A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteria.

Question 1106

An efficient use of public key infrastructure (PKI) should encrypt the:

- ☐ entire message.
- ☐ private key.
- ☐ public key.
- ☒ symmetric session key.

Explanation:

Explanation:

Public key (asymmetric) cryptographic systems require larger keys (1,024 bits) and involve intensive and time-consuming computations. In comparison, symmetric encryption is considerably faster, yet relies on the security of the process for exchanging the secret key. To enjoy the benefits of both systems, a symmetric session key is exchanged using public key methods, after which it serves as the secret key for encrypting/decrypting messages sent between two parties.

Question 1107

Am advantage of the use of hot sites as a backup alternative is that:

- ☐ the costs associated with hot sites are low.
- ☐ hot sites can be used for an extended amount of time.
- ☒ hot sites can be made ready for operation within a short period of time.
- ☐ they do not require that equipment and systems software be compatible with the primary site.

Explanation:

Explanation:

Hot sites can be made ready for operation normally within hours. However, the use of hot sites is expensive, should not be considered as a long-term solution, and requires that equipment and systems software be compatible with the primary installation being backed up.

Licensed to Berend Post berend.post@it-university.nl

Question 1108

What is the BEST population to select from when testing that programs are migrated to production with proper approval?

- ☐ List of changes provided by application programming managers
- ☐ List of production programs
- ☒ Completed change request forms
- ☐ Change advisory board meeting minutes

Question 1109

After assessing risk, the decision to treat the risk should be based PRIMARILY on:

- ☐ whether the level of risk exceeds risk appetite
- ☐ availability of financial resources
- ☐ whether the level of risk exceeds inherent risk
- ☒ the criticality of the risk

Question 1110

The BEST filter rule for protecting a network from being used as an amplifier in a denial of service (DoS) attack is to deny all:

- ☒ outgoing traffic with IP source addresses externa! to the network.
- ☐ incoming traffic with discernible spoofed IP source addresses.
- ☐ incoming traffic with IP options set.
- ☐ incoming traffic to critical hosts.

Explanation:

Explanation:

Outgoing traffic with an IP source address different than the IP range in the network is invalid, in most of the cases, it signals a DoS attack originated by an internal user or by a previously compromised internal machine; in both cases, applying this filter will stop the attack.

Question 1111

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

- ☐ Developing the CSA questionnaire
- ☐ Developing the remediation plan
- ☒ Implementing the remediation plan
- ☐ Partially completing the CSA

Licensed to Berend Post berend.post@it-university.nl

Question 1112

An IS auditor examining the configuration of an operating system to verify the controls should review the:

- ☐ transaction logs.
- ☐ authorization tables.
- ☒ parameter settings.
- ☐ routing tables.

Explanation:

Explanation:

Parameters allow a standard piece of software to be customized for diverse environments and are important in determining how a system runs. The parameter settings should be appropriate to an organization's workload and control environment, improper implementation and/or monitoring of operating systems can result in undetected errors and corruption of the data being processed, as well as lead to unauthorized access and inaccurate logging of system usage. Transaction logs are used to analyze transactions in master and/or transaction files. Authorization tables are used to verify implementation of logical access controls and will not be of much help when reviewing control features of an operating system. Routing tables do not contain information about the operating system and, therefore, provide no information to aid in the evaluation of controls.

Question 1113

An IS auditor conducting audit follow-up activities learns that some previously agreed-upon corrective actions have not been taken and that the associated risk has been accepted by senior management. If the auditor disagrees with management's decision, what is the BEST way to address the situation?

- ☐ Repeat the audit with audit scope only covering areas with accepted risks
- ☒ Report the issue to the chief audit executive for resolution
- ☐ Recommend new corrective actions to mitigate the accepted risk
- ☐ Take no action since management's decision has been made

Question 1114

Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

- ☐ PERT
- ☒ Rapid application development (RAD)
- ☐ Function point analysis (FPA)
- ☐ GANTT

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

Question 1115

An IS auditor observes an organization is performing data backup and restoration testing on an ad hoc basis without a defined process. What is the MOST likely result of a data disruption event?

- ☒ Increased loss impact
- ☐ Decreased data confidentiality
- ☐ Increased likelihood of future risk events
- ☐ Decreased data integrity

Question 1116

An organization's disaster recovery plan should address early recovery of:

- ☐ all information systems processes.
- ☐ all financial processing applications.
- ☐ only those applications designated by the IS manager.
- ☒ processing in priority order, as defined by business management.

Explanation:

Explanation:

Business management should know which systems are critical and when they need to process well in advance of a disaster. It is management's responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

Question 1117

Digital signatures require the:

- ☐ signer to have a public key and the receiver to have a private key.
- ☒ signer to have a private key and the receiver to have a public key.
- ☐ signer and receiver to have a public key.
- ☐ signer and receiver to have a private key.

Explanation:

Explanation:

Digital signatures are intended to verify to a recipient the integrity of the data and the identity of the sender. The digital signature standard is a public key algorithm. This requires the signer to have a private key and the receiver to have a public key.

Licensed to Berend Post berend.post@it-university.nl

Question 1118

Which of the following would BEST detect logic bombs in the new programs?

- ☐ Final acceptance testing by users
- ☐ Parallel/pilot testing
- ☒ Regression testing
- ☐ Independent program review

Question 1119

Which of the following is an analytical review procedure for a payroll system?

- ☐ Performing penetration attempts on the payroll system
- ☐ Evaluating the performance of the payroll system, using benchmarking software
- ☒ Performing reasonableness tests by multiplying the number of employees by the average wage rate
- ☐ Testing hours reported on time sheets

Question 1120

Which of the following should be the MOST important consideration when prioritizing the funding for competing IT projects?

- ☒ Criteria used to determine the benefits of projects
- ☐ Skills and capabilities within the project management team
- ☐ Quality and accuracy of the IT project inventory
- ☐ Senior management preferences

Question 1121

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. After the data quality team identifies the system data at fault, which of the following should internal audit recommend as the NEXT step in the process?

- ☒ Create business rules that validate data quality.
- ☐ Develop an improvement plan.
- ☐ Identify the root cause of data quality problems.
- ☐ Identify the source data owners.

Licensed to Berend Post berend.post@it-university.nl

Question 1122

An organization has decided to migrate payroll processing to a new platform hosted by a third party in a different country. Which of the following is MOST important for the IS auditor to consider?

- ☐ The service provider's compliance with privacy regulations
- ☐ Whether the contract contains a right-to-terminate clause
- ☒ The service provider's compliance with financial regulations
- ☐ Storage costs charged by the service provider

Question 1123

Which of the following controls can BEST detect accidental corruption during transmission of data across a network?

- ☐ Sequence checking
- ☒ Parity checking
- ☐ Symmetric encryption
- ☐ Check digit verification

Explanation:

Explanation:

Parity check is used to detect transmission errors in the data. When a parity check is applied to a single character, it is called vertical or column check. In addition, if a parity check is applied to all the data it is called vertical or row check. By using both types of parity check simultaneously can greatly increase the error detection possibility, which may not be possible when only one type of parity check is used.

Question 1124

An organization has outsourced some of its subprocesses to a service provider. When scoping the audit of the provider, the organization's internal auditor should FIRST:

- ☐ evaluate operational controls of the provider
- ☒ discuss audit objectives with the provider
- ☐ review internal audit reports of the provider
- ☐ review the contract with the provider

Licensed to Berend Post berend.post@it-university.nl

Question 1125

Which of the following is the MOST important requirement for the successful implementation of security governance?

- ☐ Aligning to an international security framework
- ☒ Mapping to organizational strategies
- ☐ Implementing a security balanced scorecard
- ☐ Performing an enterprise-wide risk assessment

Question 1126

Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems:

- ☐ desktop systems
- ☐ laptop systems
- ☐ handheld PDAs
- ☒ business-critical systems
- ☐ None of the choices.

Explanation:

Explanation:

Fault-tolerance enables a system to continue operating properly in the event of the failure of some parts of it. It avoids total breakdown, and is particularly sought-after in high-availability environment full of business critical systems.

Question 1127

An IS auditor is reviewing the remote access methods of a company used to access system remotely. Which of the following is LEAST preferred remote access method from a security and control point of view?

- ☐ RADIUS
- ☐ TACACS
- ☒ DIAL-UP
- ☐ DIAMETER

Explanation:

Dial-up connectivity not based on centralize control and least preferred from security and control standpoint.

Remote access user can connect remotely to their organization's networks with the same level of functionality as if they would access from within their office.

Licensed to Berend Post berend.post@it-university.nl

In connecting to an organization's network, a common method is to use dial-up lines. Access is granted through the organization's network access server (NAS) working in concert with an organization network firewall and router. The NAS handle user authentication, access control and accounting while maintaining connectivity. The most common protocol for doing this is the Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Controller System (TACACS).

Remote access Controls include:

Policy and standard

Proper authorization

Identification and authentication mechanism

Encryption tool and technique such as use of VPN

System and network management

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 334

Question 1128

When designing an incident response plan to be agreed upon with a cloud computing vendor, including which of the following will BEST help to ensure the effectiveness of the plan?

- ☐ A training program for the vendor staff
- ☐ An audit and compliance program
- ☒ Responsibility and accountability assignments
- ☐ Requirements for onsite recovery testing

Question 1129

Which of the following sampling techniques is commonly used in fraud detection when the expected occurrence rate is small and the specific controls are critical?

- ☐ Discovery sampling
- ☐ Monetary unit sampling
- ☒ Stop-or-go sampling
- ☐ Random sampling

Licensed to Berend Post berend.post@it-university.nl

Question 1130

An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the BEST way to address this situation?

- ☒ Demonstrate alignment of the information security function with business needs.
- ☐ Escalate noncompliance concerns to the internal audit manager.
- ☐ Report the risk and status of the information security program to the board.
- ☐ Revise the information security strategy to meet executive management's expectations.

Question 1131

Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

- ☐ System log analysis
- ☒ Compliance testing
- ☐ Forensic analysis
- ☐ Analytical review

Explanation:

Explanation:

Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs. Forensic analysis is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

Question 1132

An organization performs nightly backups but does not have a formal policy. An IS auditor should FIRST:

- ☒ evaluate current backup procedures
- ☐ escalate to senior management
- ☐ document a policy for the organization
- ☐ recommend automated backup

Licensed to Berend Post berend.post@it-university.nl

Question 1133

Which of the following is the PRIMARY reason for an IS auditor to use computer-assisted audit techniques (CAATs)?

- ☐ To efficiently test an entire population
- ☐ To perform direct testing of production data
- ☐ To conduct automated sampling for testing
- ☒ To enable quicker access to information

Question 1134

Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion detection system (IDS)?

- ☐ The activities being monitored deviate from what is considered normal.
- ☐ The environment is complex.
- ☒ The pattern of normal behavior changes quickly and dramatically.
- ☐ The information regarding monitored activities becomes state.

Question 1135

Which of the following should be the PRIMARY basis for planning and prioritizing IT infrastructure security audits?

- ☒ Asset value to the organization
- ☐ Management requests
- ☐ The organization's risk appetite
- ☐ Security best practice

Question 1136

An IS auditor is reviewing a bank's service level agreement (SLA) with a third-party provider that hosts the bank's secondary data center. Which of the following findings should be of GREATEST concern to the auditor?

- ☐ The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan
- ☒ The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan
- ☐ Backup data is hosted online only
- ☐ The SLA has not been reviewed in more than a year

Licensed to Berend Post berend.post@it-university.nl

Question 1137

Which of the following would BEST facilitate the detection of internal fraud perpetrated by an individual?

- ☐ Corporate fraud hotline
- ☐ Segregation of duties
- ☒ Mandatory leave
- ☐ Flexible time

Question 1138

The PRIMARY advantage of a continuous audit approach is that it:

- ☐ does not require an IS auditor to collect evidence on system reliability while processing is taking place.
- ☐ requires the IS auditor to review and follow up immediately on all information collected.
- ☒ can improve system security when used in time-sharing environments that process a large number of transactions.
- ☐ does not depend on the complexity of an organization's computer systems.

Explanation:

Explanation:

The use of continuous auditing techniques can improve system security when used in time- sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach often does require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

Question 1139

Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

- ☐ Function point analysis
- ☒ Earned value analysis
- ☐ Cost budget
- ☐ Program Evaluation and Review Technique

Explanation:

Explanation:

Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the

Licensed to Berend Post berend.post@it-university.nl

schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed, to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work breakdown structure exists. Function point analysis (FPA) is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget. Cost budgets do not address time. PERT aids in time and deliverables management, but lacks projections for estimates at completion (EACs) and overall financial management.

Question 1140

Which of the following tasks should be performed FIRST when preparing a disaster recovery plan?

- ☐ Develop a recovery strategy.
- ☒ Perform a business impact analysis.
- ☐ Map software systems, hardware and network components.
- ☐ Appoint recovery teams with defined personnel, roles and hierarchy.

Explanation:

Explanation:

The first step in any disaster recovery plan is to perform a business impact analysis. All other tasks come afterwards.

Question 1141

Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

- ☐ Release-to-release source and object comparison reports
- ☐ Library control software restricting changes to source code
- ☐ Restricted access to source code and object code
- ☒ Date and time-stamp reviews of source and object code

Explanation:

Explanation:

Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.

Licensed to Berend Post berend.post@it-university.nl

Question 1142

Labeling information according to its security classification:

- ☐ reduces the need to identify baseline controls for each classification.
- ☐ reduces the number and type of countermeasures required.
- ☐ enhances the likelihood of people handling information securely.
- ☒ affects the consequences if information is handled insecurely.

Question 1143

When conducting a penetration test of an IT system, an organization should be MOST concerned with:

- ☐ the confidentiality of the report.
- ☐ finding all possible weaknesses on the system.
- ☒ restoring all systems to the original state.
- ☐ logging all changes made to the production system.

Explanation:

Explanation:

All suggested items should be considered by the system owner before agreeing to penetration tests, but the most important task is to be able to restore all systems to their original state.

Information that is created and/or stored on the tested systems should be removed from these systems. If for some reason, at the end of the penetration test, this is not possible, all files (with their location) should be identified in the technical report so that the client's technical staff will be able to remove these after the report has been received.

Question 1144

Which of the following should an IS auditor be MOST concerned with during a post-implementation review?

- ☒ The system does not have a maintenance plan
- ☐ The system contains several minor defects
- ☐ The system was over budget by 15%
- ☐ The system deployment was delayed by three weeks

Question 1145

Which of the following is MOST likely to enable a hacker to successfully penetrate a system?

- ☐ Lack of virus protection
- ☒ Unpatched software
- ☐ Decentralized dialup access
- ☐ Lack of DoS protection

Licensed to Berend Post berend.post@it-university.nl

Question 1146

A LAN administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager.
- ☒ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Explanation:

Explanation:

A LAN administrator should not have programming responsibilities but may have end- user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

Question 1147

Which of the following is the MAIN purpose of implementing an incident response process?

- ☐ Provide substantial audit-trail evidence.
- ☐ Assign roles and responsibilities.
- ☐ Comply with policies and procedures.
- ☒ Manage impact due to breaches.

Question 1148

Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

- ☐ Degaussing
- ☒ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Explanation:

Software tools can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media.

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed. Simply deleting files or formatting media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type

Licensed to Berend Post berend.post@it-university.nl

of media on which the data resides. Specialized hardware devices known as degausses can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There exists a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. To provide higher assurance in this case, it is necessary to overwrite each sector multiple times. Security practitioners should keep in mind that a one-time pass may be acceptable for noncritical information, but sensitive data should be overwritten with multiple passes. Overwrite software can also be used to clear the sectors within solid-state media such as USB thumb drives. It is suggested that physical destruction methods such as incineration or secure recycling should be considered for solid-state media that is no longer used.

The last form of preventing unauthorized access to sensitive data is media destruction. Shredding, burning, grinding, and pulverizing are common methods of physically destroying media. Degaussing can also be a form of media destruction. High-power degausses are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal.

The following answers are incorrect:

Degaussing -Erasing data by applying magnetic field around magnetic media. Degausses device is used to erase the data. Sometime degausses can make magnetic media unusable. So degaussing is not recommended way if magnetic media needs to be reused.

Licensed to Berend Post berend.post@it-university.nl

Format magnetic media – Formatting magnetic media does not erase all data. Data can be recoverable after formatting using software tools.

Delete File allocation table-It will not erase all data. Data can be recoverable using software tools.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 338

Question 1149

Audit management has just completed the annual audit plan for the upcoming year, which consists entirely of high-risk processes. However, it is determined that there are insufficient resources to execute the plan. What should be done NEXT?

- ☐ Remove audits from the annual plan to better match the number of resources available
- ☐ Reduce the scope of the audits to better match the number of resources available
- ☒ Present the annual plan to the audit committee and ask for more resources
- ☐ Review the audit plan and defer some audits to the subsequent year

Question 1150

A major portion of what is required to address nonrepudiation is accomplished through the use of:

- ☐ strong methods for authentication and ensuring data validity
- ☒ strong methods for authentication and ensuring data integrity.
- ☐ strong methods for authorization and ensuring data integrity.
- ☐ strong methods for authentication and ensuring data reliability.
- ☐ None of the choices.

Explanation:

Explanation:

A major portion of what is required to address nonrepudiation is accomplished through the use of strong methods for authentication and ensuring data integrity.

Question 1151

Which of the following privacy principles ensures data controllers do not use personal data unintended ways that breach protection of data subjects?

- ☐ Data retention
- ☐ Adequacy
- ☐ Accuracy
- ☒ Purpose limitation

Licensed to Berend Post berend.post@it-university.nl

Question 1152

Which of the following is the MOST critical step in planning an audit?

- ☐ Implementing a prescribed auditing framework such as COBIT
- ☐ Identifying current controls
- ☒ Identifying high-risk audit targets
- ☐ Testing controls

Explanation:

Explanation:

In planning an audit, the most critical step is identifying the areas of high risk.

Question 1153

Talking about biometric authentication, physical characteristics typically include (Choose five.):

- ☒ fingerprints
- ☒ eye retinas
- ☒ irises
- ☒ facial patterns
- ☒ hand measurements
- ☐ None of the choices.

Explanation:

Explanation:

Biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes. Physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while behavioral characteristics include signature, gait and typing patterns. Voice is often considered as a mix of both physical and behavioral characteristics.

Question 1154

Which of the following is a detective control that can be used to uncover unauthorized access to information systems?

- ☐ Requiring long and complex passwords for system access
- ☒ Implementing a security information and event management (SIEM) system
- ☐ Requiring internal audit to perform periodic reviews of system access logs
- ☐ Protecting access to the data center with multifactor authentication

Licensed to Berend Post berend.post@it-university.nl

Question 1155

While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered. Which of the following control is implemented by Lily?

- ☐ Range Check
- ☒ Duplicate Check
- ☐ Existence check
- ☐ Reasonableness check

Explanation:

In a duplicate check control new transaction are matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check -Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check -Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Licensed to Berend Post berend.post@it-university.nl

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his/her date of birth.

The following were incorrect answers:

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

 Licensed to Berend Post berend.post@it-university.nl

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 215

Question 1156

Which of the following should be reviewed FIRSTwhen assessing the effectiveness of an organization's network security procedures and controls?

- ☐ Data recovery capability
- ☒ Inventory of authorized devices
- ☐ Vulnerability remediation
- ☐ Malware defenses

Question 1157

Which of the following is the BEST way to satisfy a two-factor user authentication?

- ☒ A smart card requiring the user's PIN
- ☐ User ID along with password
- ☐ Iris scanning plus fingerprint scanning
- ☐ A magnetic card requiring the user's PIN

Explanation:

Explanation:

A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). An ID and password, what the user knows, is a single-factor user authentication. Choice C is not a two- factor user authentication because it is only biometric. Choice D is similar to choice A, but the magnetic card may be copied; therefore, choice A is the best way to satisfy a two-factor user authentication.

Licensed to Berend Post berend.post@it-university.nl

Question 1158

When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?

- ☐ The security awareness programs
- ☐ Post-incident analysis results
- ☒ The risk management processes
- ☐ Firewall logs

Question 1159

A security regulation requires the disabling of direct administrator access. Such access must occur through an intermediate server that holds administrator passwords for all systems and records all actions. An IS auditor's PRIMARY concern with this solution would be that:

- ☐ it is not feasible to implement.
- ☒ it represents a single point of failure.
- ☐ segregation of duties is not observed.
- ☐ access logs may not be maintained.

Question 1160

What uses questionnaires to lead the user through a series of choices to reach a conclusion?

- ☐ Logic trees
- ☒ Decision trees
- ☐ Decision algorithms
- ☐ Logic algorithms

Explanation:

Explanation: Decision trees use questionnaires to lead the user through a series of choices to reach a conclusion.

Question 1161

Which of the following BEST describes an audit risk?

- ☒ The financial report may contain undetected material errors.
- ☐ The company is being sued for false accusations.
- ☐ Key employees have not taken vacation for 2 years.
- ☐ Employees have been misappropriating funds.

Licensed to Berend Post berend.post@it-university.nl

Question 1162

A recent audit concluded that an organization's information security system was weak and that monitoring would likely fail to detect penetration. Which of the following would be the MOST appropriate recommendation?

- ☐ Look continually for new criminal behavior and attacks on sensitive data
- ☐ Establish a clear policy related to security and the handling of sensitive data
- ☒ Encrypt sensitive data while strengthening the system
- ☐ Identify and periodically remove sensitive data that is no longer needed

Question 1163

Why does the IS auditor often review the system logs?

- ☐ To get evidence of password spoofing
- ☐ To get evidence of data copy activities
- ☒ To determine the existence of unauthorized access to data by a user or program
- ☐ To get evidence of password sharing

Explanation:

Explanation:

When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

Question 1164

Which of the following is MOST directly affected by network performance monitoring tools?

- ☐ Integrity
- ☒ Availability
- ☐ Completeness
- ☐ Confidentiality

Explanation:

Explanation:

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

Licensed to Berend Post berend.post@it-university.nl

Question 1165

Which of the following entities is BEST suited to define the data classification levels within an organization?

- ☐ Database administrator based on the data schema
- ☐ Legal compliance team based on the application regulations
- ☒ Business owner responsible for the respective data
- ☐ System administrator responsible for data security controls

Question 1166

Which of the following should be the PRIMARY basis for how digital evidence is handled during a forensics investigation?

- ☐ Industry best practices
- ☒ Regulatory requirements
- ☐ Organizational risk culture
- ☐ Established business practices

Question 1167

Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?

- ☒ Black-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application (e.g. what the software does) without peering into its internal structures or workings (see white-box testing). This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

For your exam you should know the information below:

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and

Licensed to Berend Post berend.post@it-university.nl

normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user’s desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 167

Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

Question 1168

Which of the following statement correctly describes the difference between IPSec and SSH protocols?

- ☐ IPSec works at the transport layer where as SSH works at the network layer of an OSI Model
- ☒ IPSec works at the network layer where as SSH works at the application layer of an OSI Model
- ☐ IPSec works at the network layer and SSH works at the transport layer of an OSI Model
- ☐ IPSec works at the transport layer and SSH works at the network layer of an OSI Model

Explanation:

For CISA exam you should know below information about SSH and IPSec protocol

SSH -A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including password, binary files and administrative commands, transmitted between system on a network. SSH is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation)

Licensed to Berend Post berend.post@it-university.nl

IPSec -The IP network layer packet security protocol establishes VPNsvia transport and tunnel mode encryption methods. For the transport method, the data portion of each packet referred to as the encapsulation security payload(ESP) is encrypted, achieving confidentiality over a process. In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied. In establishing IPSec sessions in either mode, Security Association (SAs) are established. SAs defines which security parameters should be applied between communication parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAsis established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host. IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and those of the cryptographic keys.

The following were incorrect answers:

The other options presented are invalid as IPSec works at network layer where as SSH works at application layer of an OSI Model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352 and 353

Question 1169

What determines the strength of a secret key within a symmetric key cryptosystem?

- ☐ A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
- ☒ A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
- ☐ A combination of key length and the complexity of the data-encryption algorithm that uses the key
- ☐ Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Explanation:

Explanation:

The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

 Licensed to Berend Post berend.post@it-university.nl

Question 1170

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

- ☐ translating and unbundling transactions.
- ☒ routing verification procedures.
- ☐ passing data to the appropriate application system.
- ☐ creating a point of receipt audit log.

Explanation:

Explanation:

The communication's interface stage requires routing verification procedures. Edi or ANSI X12 is a standard that must be interpreted by an application for transactions to be processed and then to be invoiced, paid and sent, whether they are for merchandise or services. There is no point sending and receiving EDI transactions if they cannot be processed by an internal system.

Unpacking transactions and recording audit logs are important elements that help follow business rules and establish controls, but are not part of the communication's interface stage.

Question 1171

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

- ☒ Consider feasibility of a separate user acceptance environment
- ☐ Schedule user testing to occur at a given time each day
- ☐ implement a source code version control tool
- ☐ Only retest high priority defects

Explanation:

Explanation:

A separate environment or environments is normally necessary for testing to be efficient and effective, and to ensure the integrity of production code, it is important that the development and testing code base be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing

Licensed to Berend Post berend.post@it-university.nl

covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

Question 1172

Which of the following would be MOST important to update once a decision has been made to outsource a critical application to a cloud service provider?

- ☒ Project portfolio
- ☐ IT resource plan
- ☐ IT budget
- ☐ Business impact analysis (BIA)

Question 1173

An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPIs). Which of the following findings should be of MOST concern to the auditor?

- ☐ Some KPIs are not documented.
- ☐ KPIs have never been updated.
- ☐ KPIs data is not being analyzed.
- ☒ KPIs are not clearly defined.

Question 1174

In which of the following transmission media it is MOST difficult to modify the information traveling across the network?

- ☐ Copper cable
- ☒ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Explanation:

Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Licensed to Berend Post berend.post@it-university.nl

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Licensed to Berend Post berend.post@it-university.nl

Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System

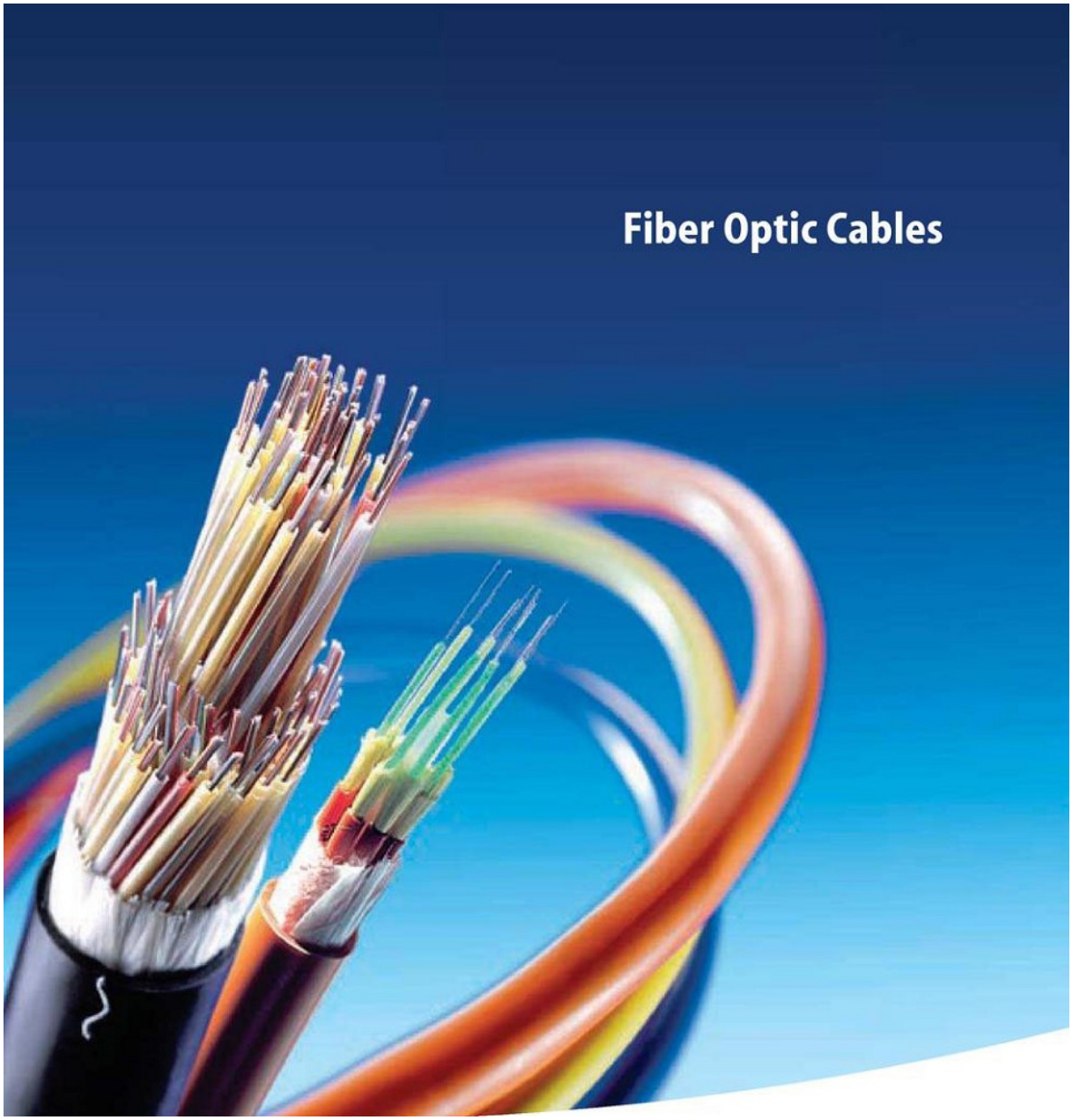
Radio systems are used for short distance, cheap and easy to tap.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

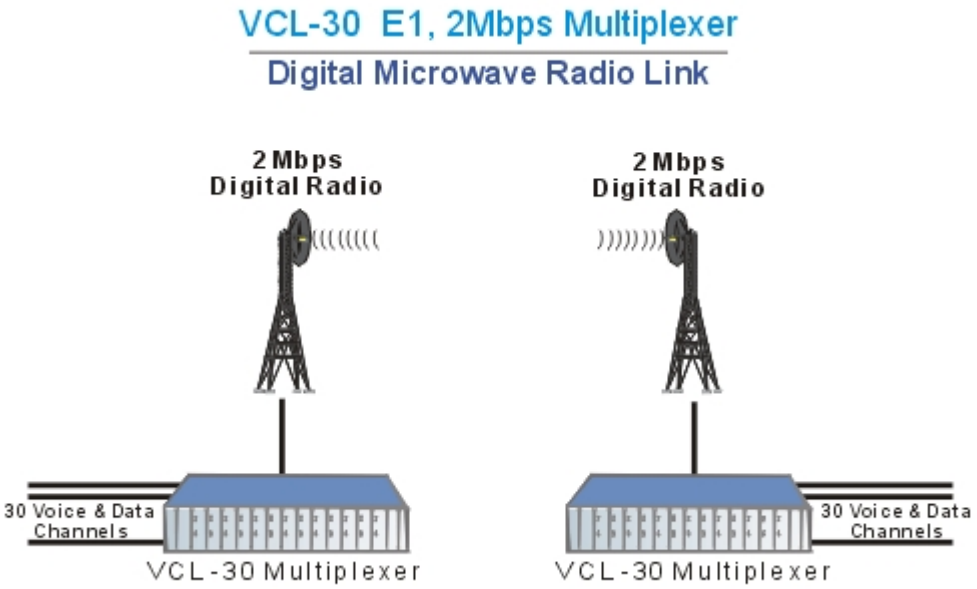
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Licensed to Berend Post berend.post@it-university.nl

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to tap.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable - Coaxial cable are expensive and does not support many LAN's. It supports data and video

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

Question 1175

The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

- ☒ duration of the outage.
- ☐ type of outage.
- ☐ probability of the outage.
- ☐ cause of the outage.

Explanation:

Explanation:

The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.

Question 1176

During an audit of an organization's incident management process, an IS auditor learns that the security operations team includes detailed reports of recent attacks in its communications to employees. Which of the following is the GREATEST concern with this situation?

- ☐ Employees may fail to understand the severity of the threats.
- ☐ The reports may be too complex for a nontechnical audience.
- ☒ Employees may misuse the information in the reports.
- ☐ There is not a documented procedure to communicate the reports.

Question 1177

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

- ☒ In program development and change management
- ☐ In program feasibility studies
- ☐ In program development
- ☐ In change management

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

Question 1178

An organization wants to reuse company-provided smartphones collected from staff leaving the organization. Which of the following would be the BEST recommendation?

- ☐ The memory cards of the smartphones should be replaced.
- ☐ Smartphones should not be reused, but physically destroyed.
- ☒ Data should be securely deleted from the smartphones.
- ☐ The SIM card and telephone number should be changed.

Question 1179

An IS auditor is evaluating the completeness of privacy procedures involving personally identifiable information (PII). Which of the following is MOST important for the auditor to verify is included in the procedures?

- ☒ Regulatory requirements for protecting PII
- ☐ The organization's definition of PII
- ☐ Encryption requirements for transmitting PII externally
- ☐ A description of how PII is masked within key systems

Question 1180

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

- ☐ interface errors are detected earlier.
- ☐ confidence in the system is achieved earlier.
- ☒ errors in critical modules are detected earlier.
- ☐ major functions and processing are tested earlier.

Explanation:

Explanation:

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach, which follows the opposite path, either in depth-first or breadth-first search order.

Licensed to Berend Post berend.post@it-university.nl

Question 1181

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- ☒ Outsourced activities are core and provide a differentiated advantage to the organization.
- ☐ Periodic renegotiation is specified in the outsourcing contract.
- ☐ The outsourcing contract fails to cover every action required by the arrangement.
- ☐ Similar activities are outsourced to more than one vendor.

Explanation:

Explanation:

An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, while multisourcing is an acceptable way to reduce risk.

Question 1182

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

- ☐ Sag
- ☐ Blackout
- ☒ Brownout
- ☐ EMI

Explanation:

The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

For CISA exam you should know below information about power failure

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Licensed to Berend Post berend.post@it-university.nl

Sags, spike and surge – Temporary and rapid decreases (sag) or increases (spike and surges) in a voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices.

Electromagnetic interference (EMI) - The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

The following were incorrect answers:

Sag – Temporarily rapid decrease in a voltage.

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number372

Question 1183

Which of the following are designed to detect network attacks in progress and assist in post- attack forensics?

- ☒ Intrusion Detection Systems
- ☐ Audit trails
- ☐ System logs
- ☐ Tripwire
- ☐ None of the choices.

Explanation:

Explanation:

Intrusion Detection Systems are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

Licensed to Berend Post berend.post@it-university.nl

Question 1184

Which of the following data would be used when performing a business impact analysis (BIA)?

- ☒ Projected impact of current business on future business
- ☐ Cost of regulatory compliance
- ☐ Cost benefit analysis of running the current business
- ☐ Expected costs for recovering the business.

Question 1185

Which of the following is penetration test where the penetration tester is provided with limited or no knowledge of the target's information systems?

- ☐ External Testing
- ☐ Internal Testing
- ☒ Blind Testing
- ☐ Targeted Testing

Explanation:

Blind Testing refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target. Such a testing is expensive, since the penetration tester has to research the target and profile it based on publicly available information.

For your exam you should know below mentioned penetration types

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system is usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such a testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Double Blind Testing -It is an extension of blind testing, since the administrator and security staff at the target are also not aware of test. Such a testing can effectively evaluate the incident handling and response capability of the target.

Licensed to Berend Post berend.post@it-university.nl

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

The following were incorrect answers:

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system is usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

The Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 369

Question 1186

Which of the following is MOST important to the successful implementation of an information security governance framework across the organization?

- ☐ The existing organizational security culture
- ☒ Security management processes aligned with security objectives
- ☐ Organizational security controls deployed in line with regulations
- ☐ Security policies that adhere to industry best practices

Licensed to Berend Post berend.post@it-university.nl

Question 1187

An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

- ☒ a data loss of up to 1 minute, but the processing must be continuous.
- ☐ a 1-minute processing interruption but cannot tolerate any data loss.
- ☐ a processing interruption of 1 minute or more.
- ☐ both a data less and processing interruption longer than 1 minute.

Explanation:

Explanation:

The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

Question 1188

The MOST efficient way to confirm that an ERP system being implemented satisfies business expectations is to utilize which of the following types of testing?

- ☐ Parallel
- ☒ Pilot
- ☐ Sociability
- ☐ Alpha

Question 1189

Which of the following would be considered an essential feature of a network management system?

- ☒ A graphical interface to map the network topology
- ☐ Capacity to interact with the Internet to solve the problems
- ☐ Connectivity to a help desk for advice on difficult issues
- ☐ An export facility for piping data to spreadsheets

Explanation:

Explanation:

To trace the topology of the network, a graphical interface would be essential. It is not necessary that each network be on the internet and connected to a help desk, while the ability to export to a spreadsheet is not an essential element.

Licensed to Berend Post berend.post@it-university.nl

Question 1190

The business owner's approval of software changes being moved into production is PRIMARILY necessary to:

- ☒ ensure that an application functionality requirement is satisfied.
- ☐ prevent unauthorized access to data.
- ☐ inform management of deployments of new functionality.
- ☐ confirm there is a process to control system changes.

Question 1191

Which of the following is a reason for implementing a decentralized IT governance model?

- ☐ Standardized controls and economies of scale
- ☐ IT synergy among business units
- ☐ Greater consistency among business units
- ☒ Greater responsiveness to business needs

Question 1192

Which of the following would BEST provide assurance of the integrity of new staff?

- ☒ background screening
- ☐ References
- ☐ Bonding
- ☐ Qualifications listed on a resume

Explanation:

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

Question 1193

Which of the following would be of GREATEST concern to an IS auditor evaluating governance over open source development components?

- ☐ The development project has gone over budget and time
- ☐ The open source development components do not meet industry best practices
- ☒ The software is not analyzed for compliance with organizational requirements
- ☐ Existing open source policies have not been approved in over a year

Licensed to Berend Post berend.post@it-university.nl

Question 1194

An employee has accidentally posted confidential data to the company's social media page. Which of the following is the BEST control to prevent this from recurring?

- ☐ Require all updates to be made by the marketing director
- ☒ Implement a moderator approval process
- ☐ Perform periodic audits of social media updates
- ☐ Establish two-factor access control for social media accounts

Question 1195

During a review of a production schedule, an IS auditor observes that a staff member is not complying with mandatory operational procedures. The auditor's NEXT step should be to:

- ☒ determine why the procedures were not followed.
- ☐ include the noncompliance in the audit report.
- ☐ note the noncompliance in the audit working papers.
- ☐ issue an audit memorandum identifying the noncompliance.

Question 1196

Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

- ☒ it improves security at a cost in functionality.
- ☐ it improves functionality at a cost in security.
- ☐ it improves security at a cost in system performance.
- ☐ it improves performance at a cost in functionality.
- ☐ None of the choices.

Explanation:

Explanation:

"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality. This is a good approach if you have lots of security threats. On the other hand, ""Everything not explicitly forbidden is permitted"" (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non-existent or negligible."

Licensed to Berend Post berend.post@it-university.nl

Question 1197

At a project steering committee meeting, it is stated that adding controls to business processes undergoing re-engineering is an unnecessary cost. The IS auditor's BEST response is that the actual control overhead for a business process is:

- ☐ usually considerable, but the benefits of good controls always exceed the cost.
- ☐ the responsibility of the project manager, and the cost should have been included in the budget.
- ☐ usually difficult to ascertain but is justifiable, because controls are essential to doing business
- ☒ usually less than the potential cost of failure caused by lack of controls.

Question 1198

An advantage of installing a thin client architecture in a local area network (LAN) is that this would:

- ☐ stabilize network bandwidth requirements
- ☒ facilitate the updating of software versions
- ☐ ensure application availability when the server is down
- ☐ reduce the risk of a single point of failure

Question 1199

An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?

- ☐ Monitor and notify IT staff of critical patches.
- ☒ Evaluate patch management training.
- ☐ Perform regular audits on the implementation of critical patches.
- ☐ Assess the patch management process.

Question 1200

Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

- ☐ Intrusion detection systems
- ☒ Data mining techniques
- ☐ Firewalls
- ☐ Packet filtering routers

Explanation:

Explanation:

Data mining is a technique used to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

Licensed to Berend Post berend.post@it-university.nl

Question 1201

The GREATEST benefit of choosing a private cloud over a public cloud would be:

- ☐ server protection.
- ☐ online service availability.
- ☒ containment of customer data.
- ☐ collection of data forensics.

Question 1202

During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

- ☐ Recommend redesigning the change management process.
- ☒ Gain more assurance on the findings through root cause analysis.
- ☐ Recommend that program migration be stopped until the change process is documented.
- ☐ Document the finding and present it to management.

Explanation:

Explanation:

A change management process is critical to IT production systems. Before recommending that the organization take any other action (e.g., stopping migrations, redesigning the change management process), the IS auditor should gain assurance that the incidents reported are related to deficiencies in the change management process and not caused by some process other than change management.

Question 1203

Which of the following type of network service maps Domain Names to network IP addresses or network IP addresses to Domain Names?

- ☐ DHCP
- ☒ DNS
- ☐ Directory Service
- ☐ Network Management

Explanation:

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

For your exam you should know below information about network services:

Licensed to Berend Post berend.post@it-university.nl

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine.

Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:

Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.

Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.

Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Question 1204

Which of the following is an implementation risk within the process of decision support systems?

- ☐ Management control
- ☐ Semistructured dimensions
- ☒ inability to specify purpose and usage patterns
- ☐ Changes in decision processes

Explanation:

Explanation:

The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DDS.

Licensed to Berend Post berend.post@it-university.nl

Question 1205

Identify the correct sequence of Business Process Reengineering (BPR) application steps from the given choices below?

- ☒ Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Initiate, Envision, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Envision, Diagnose, Initiate, Redesign, Reconstruct and Evaluate
- ☐ Evaluate, Envision, Initiate, Diagnose, Redesign, Reconstruct

Explanation:

The correct sequence of BRP application step is Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate.

For your exam you should know the information below:

Overview of Business Process Reengineering

One of the principles in business that remains constant is the need to improve your processes and procedures. Most trade magazines today contain discussions of the detailed planning necessary for implementing change in an organization. The concept of change must be accepted as a fundamental principle. Terms such as business evolution and continuous improvement ricochet around the room in business meetings. It's a fact that organizations which fail to change are destined to perish.

As a CISA, you must be prepared to investigate whether process changes within the organization are accounted for with proper documentation. All internal control frameworks require that management be held responsible for safeguarding all the assets belonging to their organization. Management is also responsible for increasing revenue.

BPR Application Steps

ISACA cites six basic steps in their general approach to BPR. These six steps are simply an extension of Stewart's Plan-Do-Check-Act model for managing projects:

Envision -Visualize a need (envision). Develop an estimate of the ROI created by the proposed change. Elaborate on the benefit with a preliminary project plan to gain sponsorship from the organization. The plan should define the areas to be reviewed and clarify the desired result at the end of the project (aka end state objective). The deliverables of the envision phase include the following:

Project champion working with the steering committee to gain top management approval

Brief description of project scope, goals, and objectives description of the specific deliverables from this project with a preliminary charter to evidence management's approval, the project may proceed into the initiation phase.

Licensed to Berend Post berend.post@it-university.nl

Initiate -This phase involves setting BPR goals with the sponsor. Focus on planning the collection of detailed evidence necessary to build the subsequent BPR plan for redesigning the process. Deliverables in the initiation phase include the following:

Identifying internal and external requirements (project specifications)

Business case explaining why this project makes sense (justification) and the estimated return on investment compared to the total cost (net ROI)

Formal project plan with budget, schedule, staffing plan, procurement plan, deliverables, and project risk analysis

Level of authority the BPR project manager will hold and the composition of any support committee or task force that will be required

From the profit and loss (P&L) statement, identify the item line number that money will be debited from to pay for this project and identify the specific P&L line number that the financial return will later appear under (to provide strict monitoring of the ROI performance)

Formal project charter signed by the sponsors

It's important to realize that some BPR projects will proceed to their planned conclusion and others may be halted because of insufficient evidence. After a plan is formally approved, the

BPR project may proceed to the diagnostic phase.

Diagnose Document existing processes. Now it's time to see what is working and identify the source of each requirement. Each process step is reviewed to calculate the value it creates. The goal of the diagnostic phase is to gain a better understanding of existing processes. The data collected in the diagnostic phase forms the basis of all planning decisions:

Detailed documentation of the existing process

Performance measurement of individual steps in the process

Evidence of specific process steps that add customer value

Identification of process steps that don't add value

Definition of attributes that create value and quality

Put in the extra effort to do a good job of collecting and analyzing the evidence. All future assumptions will be based on evidence from the diagnostic phase.

Redesign- Using the evidence from the diagnostic phase, it's time to develop the new process.

Licensed to Berend Post berend.post@it-university.nl

This will take several planning iterations to ensure that the strategic objectives are met. The formal redesign plans will be reviewed by sponsors and stakeholders. A final plan will be presented to the steering committee for approval. Here's an example of deliverables from the redesign phase.

Comparison of the envisioned objective to actual specifications

Analysis of alternatives (AoA)

Prototyping and testing of the redesigned process

Formal documentation of the final design

The project will need formal approval to proceed into the reconstruction phase. Otherwise, the redesign is halted pending further scrutiny while comparing the proposed design with available evidence. Insufficient evidence warrants halting the project.

Reconstruct With formal approval received, it's time to begin the implementation phase.

The current processes are deconstructed and reassembled according to the plan. Reconstruction may be in the form of a parallel process, modular changes, or complete transition. Each method presents a unique risk and reward opportunity. Deliverables from this phase include the following:

Conversion plan with dependencies in time sequence

Change control management

Execution of conversion plan with progress monitoring

Training of users and support personnel

Pilot implementation to ensure a smooth migration

Formal approval by the sponsor.

The reconstructed process must be formally approved by management to witness their consent for fitness of use. IT governance dictates that executive management shall be held responsible for any failures and receive recognition for exceptional results. System performance will be evaluated again after entering production use.

Evaluate (post evaluation) The reconstructed process is monitored to ensure that it works and is producing the strategic value as forecast in the original justification.

Comparison of original forecast to actual performance Identification of lessons learned

Total quality management plan to maintain the new process

Licensed to Berend Post berend.post@it-university.nl

A method of continuous improvement is implemented to track the original goals against actual process performance. Annual reevaluation is needed to adapt new requirements or new opportunities.

Benchmarking as a BPR Tool

Benchmarking is the process of comparing performance data (aka metrics). It can be used to evaluate business processes that are under consideration for reengineering. Performance data may be obtained by using a self-assessment or by auditing for compliance against a standard (reference standard). Evidence captured during the diagnostic phase is considered the key to identifying areas for performance improvement and documenting obstacles. ISACA offers the following general guidelines for performing benchmarks:

Plan Identify the critical processes and create measurement techniques to grade the processes.

Research Use information about the process and collect regular data (samples) to build a baseline for comparison. Consider input from your customers and use analogous data from other industries.

Observe Gather internal data and external data from a benchmark partner to aid the comparison results. Benchmark data can also be compared against published standards.

Analyze Look for root cause-effect relationships and other dependencies in the process. Use predefined tools and procedures to collate the data collected from all available sources.

Adapt Translate the findings into hypotheses of how these findings will help or hurt strategic business goals. Design a pilot test to prove or disprove the hypotheses.

Improve Implement a prototype of the new processes. Study the impact and note any unexpected results. Revise the process by using controlled change management. Measure the process results again. Use reestablished procedures such as total quality management for continuous improvement.

The following answers are incorrect:

The other options specified does not represent the correct sequence of BRP application steps.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 219 to 211

CISA certified information system auditor study guide Second Edition Page Number 154 to 158

Licensed to Berend Post berend.post@it-university.nl

Question 1206

Machines that operate as a closed system can NEVER be eavesdropped.

- ☐ True
- ☒ False

Explanation:

Explanation:

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

Question 1207

During a vulnerability assessment, an IS auditor finds a high-risk vulnerability in a public-facing web server used to process online customer orders via credit card. The IS auditor should FIRST:

- ☐ notify management.
- ☐ redesign the customer order process.
- ☒ document the finding in the report.
- ☐ suspend credit card processing.

Question 1208

An information security manager is developing evidence preservation procedures for an incident response plan. Which of the following would be the BEST source of guidance for requirements associated with the procedures?

- ☐ IT management
- ☐ Executive management
- ☐ Legal counsel
- ☒ Data owners

Question 1209

Which of the following findings would be of MOST concern to an IS auditor performing a review of an end-user developed application that generates financial statements?

- ☐ The application is not sufficiently supported by the IT department
- ☐ There is not adequate training in the use of the application
- ☐ There is no adequate user license for the application
- ☒ There is no control to ensure accuracy of the processed data

Licensed to Berend Post berend.post@it-university.nl

Question 1210

When reviewing the effectiveness of data center operations, the IS auditor would FIRST establish that system performance:

- ☐ is monitored and reported against agreed service levels.
- ☐ reflects the expected usage levels established at implementation.
- ☐ meets the expected targets specified by the manufacturer.
- ☒ is within generally accepted reliability levels for that system.

Question 1211

Naming conventions for system resources are important for access control because they:

- ☐ ensure that resource names are not ambiguous.
- ☒ reduce the number of rules required to adequately protect resources.
- ☐ ensure that user access to resources is clearly and uniquely identified.
- ☐ ensure that internationally recognized names are used to protect resources.

Explanation:

Explanation: Naming conventions for system resources are important for the efficient administration of security controls. The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

Question 1212

The FIRSTstep in establishing an information security program is to:

- ☒ secure organizational commitment and support
- ☐ assess the organization's compliance with regulatory requirements
- ☐ determine the level of risk that is acceptable to senior management
- ☐ define policies and standards that mitigate the organization's risks

Licensed to Berend Post berend.post@it-university.nl

Question 1213

When providing a vendor with data containing personally identifiable information (PII) for offsite testing, the data should be:

- ☐ current
- ☒ encrypted.
- ☐ sanitized.
- ☐ backed up.

Question 1214

Which of the following is MOST important for an IS auditor to consider when evaluating a Software as a Service (SaaS) arrangement?

- ☐ Total cost of ownership
- ☐ Frequency of software updates
- ☐ Physical security
- ☒ Software availability

Question 1215

Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

- ☒ Resuming critical processes
- ☐ Recovering sensitive processes
- ☐ Restoring the site
- ☐ Relocating operations to an alternative site

Explanation:

Explanation:

The resumption of critical processes has the highest priority as it enables business processes to begin immediately after the interruption and not later than the declared mean time between failure (MTBF). Recovery of sensitive processes refers to recovering the vital and sensitive processes that can be performed manually at a tolerable cost for an extended period of time and those that are not marked as high priority. Repairing and restoring the site to original status and resuming the business operations are time consuming operations and are not the highest priority. Relocating operations to an alternative site, either temporarily or permanently depending on the interruption, is a time consuming process; moreover, relocation may not be required.

Licensed to Berend Post berend.post@it-university.nl

Question 1216

The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

- ☒ Reliability and quality of service (QoS)
- ☐ Means of authentication
- ☐ Privacy of voice transmissions
- ☐ Confidentiality of data transmissions

Explanation:

Explanation:

The company currently has a VPN; issues such as authentication and confidentiality have been implemented by the VPN using tunneling. Privacy of voice transmissions is provided by the VPN protocol. Reliability and QoS are, therefore, the primary considerations to be addressed.

Question 1217

What is the best defense against Local DoS attacks?

- ☐ patch your systems.
- ☐ run a virus checker.
- ☐ run an anti-spy software.
- ☒ find this program and kill it.
- ☐ None of the choices.

Explanation:

Explanation:

Local DoS attacks can be a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files. The best defense is to find this program and kill it.

Question 1218

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

- ☐ DES
- ☒ AES
- ☐ Triple DES
- ☐ RSA

Explanation:

Explanation:

Advanced Encryption Standard (AES), a public algorithm that supports keys from 128 to 256 bits in size, not only provides good security, but provides speed and versatility across a variety of computer platforms. AES runs securely and efficiently on large computers, desktop computers and even small

Licensed to Berend Post berend.post@it-university.nl

devices such as smart cards. DES is not considered a strong cryptographic solution since its entire key space can be brute forced by large computer systems within a relatively short period of time. Triple DES can take up to three times longer than DES to perform encryption and decryption. RSA keys are large numbers that are suitable only for short messages, such as the creation of a digital signature.

Question 1219

Which of the following would BEST maintain the integrity of a firewall log?

- ☐ Granting access to log information only to administrators
- ☐ Capturing log events in the operating system layer
- ☐ Writing dual logs onto separate storage media
- ☒ Sending log information to a dedicated third-party log server

Explanation:

Explanation:

Establishing a dedicated third-party log server and logging events in it is the best procedure for maintaining the integrity of a firewall log. When access control to the log server is adequately maintained, the risk of unauthorized log modification will be mitigated, therefore improving the integrity of log information. To enforce segregation of duties, administrators should not have access to log files. This primarily contributes to the assurance of confidentiality rather than integrity. There are many ways to capture log information: through the application layer, network layer, operating systems layer, etc.; however, there is no log integrity advantage in capturing events in the operating systems layer. If it is a highly mission-critical information system, it may be nice to run the system with a dual log mode. Having logs in two different storage devices will primarily contribute to the assurance of the availability of log information, rather than to maintaining its integrity.

Question 1220

An IS auditor has obtained a large data set containing multiple fields and non-numeric data for analysis. Which of the following activities will MOST improve the quality of conclusions derived from the use of a data analytics tool for this audit?

- ☐ Data anonymization
- ☐ Data classification
- ☒ Data stratification
- ☐ Data preparation

Licensed to Berend Post berend.post@it-university.nl

Question 1221

In an environment where most IT services have been outsourced, continuity planning is BEST controlled by:

- ☐ outsourced service provider management.
- ☐ business management.
- ☒ continuity planning specialists.
- ☐ IT management.

Question 1222

In an organization that has a staff-rotation policy, the MOST appropriate access control model is:

- ☒ role based.
- ☐ discretionary.
- ☐ mandatory.
- ☐ lattice based.

Question 1223

To ensure the integrity of a recovered database, which of the following would be MOST useful?

- ☒ Before-and-after transaction images
- ☐ Database defragmentation tools
- ☐ A copy of the data dictionary
- ☐ Application transaction logs

Question 1224

Which of the following is the MOST important security consideration when using infrastructure as a Service (IaaS)?

- ☒ User access management
- ☐ Compliance with internal standards
- ☐ Segmentation among guests
- ☐ Backup and recovery strategy

Question 1225

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

- ☐ Legal
- ☐ Help desk
- ☐ Human resources
- ☒ Information security

Licensed to Berend Post berend.post@it-university.nl

Question 1226

What is the PRIMARY advantage of prototyping as part of systems development?

- ☐ Maximizes user satisfaction
- ☐ Eliminates the need for internal controls
- ☒ Increases accuracy in reporting
- ☐ Reduces the need for compliance testing

Question 1227

An IS auditor reviewed the business case for a proposed investment to virtualize an organization's server infrastructure. Which of the following is MOST likely to be included among the benefits in the project proposal?

- ☐ Fewer operating system licenses
- ☐ Better efficiency of logical resources
- ☒ Reduced hardware footprint
- ☐ Less memory and storage space

Question 1228

An organization establishes an internal document collaboration site. To ensure data confidentiality of each project group, it is MOST important to:

- ☐ conduct a vulnerability assessment.
- ☐ enforce document life cycle management.
- ☐ prohibit remote access to the site.
- ☒ periodically recertify access rights.

Question 1229

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

- ☒ Traffic analysis
- ☐ SYN flood
- ☐ Denial of service (DoS)
- ☐ Distributed denial of service (DoS)

Explanation:

Explanation:

Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

Licensed to Berend Post berend.post@it-university.nl

Question 1230

Spreadsheets are used to calculate project cost estimates. Totals for each cost category are then keyed into the job-costing system. What is the BEST control to ensure that data are accurately entered into the system?

- ☐ Reasonableness checks for each cost type
- ☐ Validity checks, preventing entry of character data
- ☐ Display back of project detail after entry
- ☒ Reconciliation of total amounts by project

Question 1231

Which of the following would be MOST time and cost efficient when performing a control self-assessment (CSA) for an organization with a large number of widely dispersed employees?

- ☐ Top-down and bottom-up analysis
- ☐ Face-to-face interviews
- ☒ Survey questionnaire
- ☐ Facilitated workshops

Question 1232

The selection of security controls is PRIMARILY linked to:

- ☐ risk appetite of the organization.
- ☐ regulatory requirements.
- ☒ business impact assessment.
- ☐ best practices of similar organizations.

Question 1233

Of the following procedures for testing a disaster recovery plan (DRP), which should be used MOST frequently?

- ☐ Unannounced shutdown of the primary computing facility.
- ☒ Review of documented backup and recovery procedures
- ☐ Testing at a secondary site using offsite data backups
- ☐ Preplanned shutdown of the computing facility during an off-peak period

Licensed to Berend Post berend.post@it-university.nl

Question 1234

Which of the following is MOST critical to the success of an information security program?

- ☒ Integration of business and information security
- ☐ Alignment of information security with IT objectives
- ☐ Management's commitment to information security
- ☐ User accountability for information security

Question 1235

How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

- ☐ By implementing redundant systems and applications onsite
- ☒ By geographically dispersing resources
- ☐ By retaining onsite data backup in fireproof vaults
- ☐ By preparing BCP and DRP documents for commonly identified disasters

Explanation:

Explanation:

Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

Question 1236

The human resources (HR) department has developed a system to allow employees to enroll in benefits via a web site on the corporate Intranet. Which of the following would protect the confidentiality of the data?

- ☒ SSL encryption
- ☐ Two-factor authentication
- ☐ Encrypted session cookies
- ☐ IP address verification

Explanation:

Explanation:

The main risk in this scenario is confidentiality, therefore the only option which would provide confidentiality is Secure Socket Layer (SSL) encryption. The remaining options deal with authentication issues.

Licensed to Berend Post berend.post@it-university.nl

Question 1237

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

- ☐ There are a number of external modems connected to the network.
- ☐ Users can install software on their desktops.
- ☐ Network monitoring is very limited.
- ☒ Many user IDs have identical passwords.

Explanation:

Explanation:

Exploitation of a known user ID and password requires minimal technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user IDs have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high {for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

Question 1238

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

- ☒ continuous improvement.
- ☐ quantitative quality goals.
- ☐ a documented process.
- ☐ a process tailored to specific projects.

Explanation:

Explanation:

An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

Licensed to Berend Post berend.post@it-university.nl

Question 1239

On a daily basis, an in-house development team moves duplicate copies of production data containing personally identifiable information (PII) to the test environment. Which of the following is the BEST way to mitigate the privacy risk involved?

- ☐ Require data owners to sign off on production data.
- ☒ Encrypt the data file.
- ☐ Obtain customer opt-in acceptances.
- ☐ Sanitize the data in the test environment.

Question 1240

As an auditor it is very important to ensure confidentiality, integrity, authenticity and availability are implemented appropriately in an information system. Which of the following definitions incorrectly describes these parameters?

1. Authenticity – A third party must be able to verify that the content of a message has been sent by a specific entity and nobody else.

2. Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

3. Accountability – The action of an entity must be uniquely traceable to different entities
4. Availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

- ☐ All of the options presented
- ☐ None of the options presented
- ☐ Options number 1 and 2
- ☒ Option number 3

Explanation:

It is important to read carefully the question. The word "incorrectly" was the key word. You had to find which one of the definitions presented is incorrect. The definition of Accountability was NOT properly described. Below you have the proper definition.

The correct definitions are as follows

Authenticity – A third party must be able to verify that the content of a message is from a specific entity and nobody else.

Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

Licensed to Berend Post berend.post@it-university.nl

Accountability – The action of an entity must be uniquely traceable to that entity

Network availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 34

Question 1241

You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?

- ☐ exploit
- ☒ vulnerability
- ☐ both

Explanation:

Explanation:

You should know the difference between an exploit and a vulnerability. An exploit refers to software, data, or commands capable of taking advantage of a bug, glitch or vulnerability in order to cause unintended behavior. Vulnerability in this sense refers to a weakness in the system.

Question 1242

The waterfall life cycle model of software development is most appropriately used when:

- ☒ requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
- ☐ requirements are well understood and the project is subject to time pressures.
- ☐ the project intends to apply an object-oriented design and programming approach.
- ☐ the project will involve the use of new technology.

Explanation:

Explanation:

Historically, the waterfall model has been best suited to the stable conditions described in choice

A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. The ability to deliver working software earlier also acts to alleviate uncertainty and may allow an

 Licensed to Berend Post berend.post@it-university.nl

earlier realization of benefits. The choice of a design and programming approach is not itself a determining factor of the type of software development life cycle that is appropriate. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

Question 1243

Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

- ☐ virus
- ☐ worm
- ☒ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ None of the choices.

Question 1244

An IS auditor is performing a business continuity plan (BCP) audit and identifies that the plan has not been tested for five years. However, the plan was successfully activated during a recent extended power outage. Which of the following is the IS auditor's BEST course of action?

- ☐ Determine if lessons learned from the activation were incorporated into the plan.
- ☐ Determine if the business impact analysis (BIA) is still accurate.
- ☒ Determine if a follow-up BCP audit is required to identify future gaps.
- ☐ Determine if the annual BCP training program is in need of a review.

Question 1245

Which of the following is MOST important for the improvement of an organization's incident response processes?

- ☒ Post-event reviews by the incident response team
- ☐ Regular upgrades to incident management software
- ☐ Ongoing incident response training for users
- ☐ Periodic walk-through of incident response procedures

Licensed to Berend Post berend.post@it-university.nl

Question 1246

An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

- ☐ source documentation retention.
- ☐ data file security.
- ☒ version usage control.
- ☐ one-for-one checking.

Explanation:

Explanation:

For processing to be correct, it is essential that the proper version of a file is used. Transactions should be applied to the most current database, while restart procedures should use earlier versions. Source documentation should be retained for an adequate time period to enable documentation retrieval, reconstruction or verification of data, but it does not aid in ensuring that the correct version of a file will be used. Data file security controls prevent access by unauthorized users who could then alter the data files; however, it does not ensure that the correct file will be used. It is necessary to ensure that all documents have been received for processing, one-for-one; however, this does not ensure the use of the correct file.

Question 1247

Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:

- ☐ almost always less efficient.
- ☐ almost always less effective.
- ☐ almost always less secure.
- ☐ almost always less costly to setup.
- ☒ None of the choices.

Explanation:

Explanation:

Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU processing power.

Packet filters operate at the network layer and function more efficiently because they only look at the header part of a packet. NO FIREWALL operates at the physical level.

Licensed to Berend Post berend.post@it-university.nl

Question 1248

Which of the following is used to evaluate biometric access controls?

- ☐ FAR
- ☒ EER
- ☐ ERR
- ☐ FRR

Explanation:

Explanation:

When evaluating biometric access controls, a low equal error rate (EER) is preferred. EER is also called the crossover error rate (CER).

Question 1249

An IS auditor has completed a review of an outsourcing agreement and has identified IT governance issues. Which of the following is the MOST effective and efficient way of communicating the issues at a meeting with senior management?

- ☐ Present a completed report and discuss the details.
- ☐ Provide a detailed report in advance and open the floor to questions.
- ☒ Present an overview highlighting the key findings.
- ☐ Provide a plan of action and milestones.

Question 1250

Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- ☒ Financial impact per security incident
- ☐ Number of security vulnerabilities that were patched
- ☐ Percentage of business applications that are being protected
- ☐ Number of successful penetration tests

Explanation:

Explanation:

The most important indicator is the financial impact per security incident. Choices B, C and D could be measures of effectiveness of security, but would not be a measure of the effectiveness of a response team.

Licensed to Berend Post berend.post@it-university.nl

Question 1251

When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

- ☐ Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
- ☒ All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
- ☐ Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
- ☐ The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Explanation:

Explanation:

Deleting and formatting does not completely erase the data but only marks the sectors that contained files as being free. There are tools available over the Internet which allow one to reconstruct most of a hard disk's contents. Overwriting a hard disk at the sector level would completely erase data, directories, indices and master file tables. Reformatting is not necessary since all contents are destroyed. Overwriting several times makes useless some forensic measures which are able to reconstruct former contents of newly overwritten sectors by analyzing special magnetic features of the platter's surface. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted. Reconstructing data would be extremely expensive since all analysis must be performed under a clean room atmosphere and is only possible within a short time frame or until the surface is corroded. Data reconstruction from shredded hard disks is virtually impossible, especially when the scrap is mixed with other metal parts. If the transport can be secured and the destruction be proved as described in the option, this is a valid method of disposal.

Question 1252

When consolidating several applications from two outdated servers onto one new server, which of the following is the GREATEST concern?

- ☐ Increased software licensing cost
- ☒ Maintenance requires more coordination
- ☐ Decreased utilization of capacity
- ☐ Increased network traffic

Licensed to Berend Post berend.post@it-university.nl

Question 1253

Which of the following is the PRIMARY reason social media has become a popular target for attack?

- ☒ The accessibility of social media from multiple locations
- ☐ The prevalence of strong perimeter protection
- ☐ The reduced effectiveness of access controls
- ☐ The element of trust created by social media

Question 1254

Which of the following is an example of a preventive control in an accounts payable system?

- ☒ The system only allows payments to vendors who are included in the system's master vendor list.
- ☐ Policies and procedures are clearly communicated to all members of the accounts payable department.
- ☐ The system produces daily payment summary reports that staff use to compare against invoice totals.
- ☐ Backups of the system and its data are performed on a nightly basis and tested periodically.

Question 1255

Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- ☒ Review the parameter settings.
- ☐ Interview the firewall administrator.
- ☐ Review the actual procedures.
- ☐ Review the device's log file for recent attacks.

Explanation:

Explanation:

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide audit evidence as strong as choice A.

Licensed to Berend Post berend.post@it-university.nl

Question 1256

Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?

- ☐ Enhanced forensic analysis
- ☒ Improved response time to incidents
- ☐ Improved network protection
- ☐ Reduced need for manual analysis

Question 1257

Which of the following procedures should an IS auditor complete FISRT when evaluating the adequacy of IT key performance indicators (KPIs)?

- ☐ Independently calculate the accuracy of the KPIs.
- ☐ Review KPIs that indicate poor IT performance.
- ☐ Validate the KPI thresholds.
- ☒ Determine whether the KPIs support IT objectives.

Question 1258

Two servers are deployed in a cluster to run a mission-critical application. To determine whether the system has been designed for optimal efficiency, the IS auditor should verify that:

- ☐ the security features in the operating system are all enabled
- ☐ the number of disks in the cluster meets minimum requirements
- ☐ the two servers are of exactly the same configuration
- ☒ load balancing between the servers has been implemented

Question 1259

An IS auditor is reviewing the performance outcomes of controls in an agile development project. Which of the following would provide the MOST relevant evidence for the auditor to consider?

- ☒ Progress report of outstanding work
- ☐ Product backlog
- ☐ Number of failed builds
- ☐ Composition of the scrum team

Licensed to Berend Post berend.post@it-university.nl

Question 1260

A legacy application is running on an operating system that is no longer supported by the vendor. If the organization continues to use the current application, which of the following should be the IS auditor's GREATEST concern?

- ☒ Potential exploitation of zero-day vulnerabilities in the system
- ☐ Inability to update the legacy application database
- ☐ Increased cost of maintaining the system
- ☐ Inability to use the operating system due to potential license issues

Question 1261

Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

- ☐ change the company's security policy.
- ☐ educate users about the risk of weak passwords.
- ☒ build in validations to prevent this during user creation and password change.
- ☐ require a periodic review of matching user ID and passwords for detection and correction.

Explanation:

Explanation:

The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

Question 1262

During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What should the auditor do FIRST?

- ☒ Discuss potential regulatory issues with the legal department.
- ☐ Ask management why the regulatory changes have not been included.
- ☐ Exclude recent regulatory changes from the audit scope.
- ☐ Report the missing regulatory updates to the chief information officer (CIO).

Licensed to Berend Post berend.post@it-university.nl

Question 1263

Which of the following is the MOST important for an IS auditor to do during an exit meeting with an auditee?

- ☒ Ensure that the facts presented in the report are correct.
- ☐ Specify implementation dates for the recommendations.
- ☐ Request input in determining corrective action.
- ☐ Communicate the recommendations to senior management.

Question 1264

The PRIMARY purpose of aligning information security with corporate governance objectives is to:

- ☐ identify an organization's tolerance for risk.
- ☐ re-align roles and responsibilities.
- ☒ build capabilities to improve security processes.
- ☐ consistently manage significant areas of risk.

Question 1265

Structured programming is BEST described as a technique that:

- ☐ provides knowledge of program functions to other programmers via peer reviews.
- ☒ reduces the maintenance time of programs by the use of small-scale program modules.
- ☐ makes the readable coding reflect as closely as possible the dynamic execution of the program.
- ☐ controls the coding and testing of the high-level functions of the program in the development process.

Explanation:

Explanation:

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well-known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

Licensed to Berend Post berend.post@it-university.nl

Question 1266

In a typical network architecture used for e-commerce, a load balancer is normally found between the:

- ☒ routers and the web servers.
- ☐ mail servers and the mail repositories.
- ☐ users and the external gateways.
- ☐ databases and the external gateways.

Question 1267

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

- ☐ Use of a cryptographic hashing algorithm
- ☐ Enciphering the message digest
- ☐ Deciphering the message digest
- ☒ A sequence number and time stamp

Explanation:

Explanation:

When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection, and could be used to verify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

Question 1268

During an IS audit of a data center, it was found that programmers are allowed to make emergency fixes to operational programs. Which of the following should be the IS auditor's PRIMARY recommendation?

- ☐ Bypass use ID procedures should be put in place to ensure that the changes are subject to after-the-event approval and testing
- ☒ The ability to undertake emergency fixes should be restricted to selected key personnel
- ☐ Programmers should be allowed to implement emergency fixes only after obtaining verbal agreement from the application owner
- ☐ Emergency program changes should be subject to program migration and testing procedures before they are applied to operational systems

Licensed to Berend Post berend.post@it-university.nl

Question 1269

Which of the following is the MOST important reason to document information security incidents that are reported across the organization?

- ☒ Prevent incident recurrence.
- ☐ Support business investments in security.
- ☐ Identify unmitigated risk.
- ☐ Evaluate the security posture of the organization.

Question 1270

An employee transfers from an organization's risk management department to become the lead IS auditor. While in the risk management department, the employee helped develop the key performance indicators (KPIs) now used by the organization. Which of the following would pose the GREATEST threat to the independence of this auditor?

- ☐ Evaluating the effectiveness of IT risk management processes
- ☒ Recommending controls to address the IT risks identified by KPIs
- ☐ Developing KPIs to measure the internal audit team
- ☐ Training the IT audit team on IT risk management processes

Question 1271

Which of the following is the BEST way to determine if IT is delivering value to the business?

- ☐ Distribute surveys to various end users of IT services.
- ☐ Interview key IT managers and service providers.
- ☒ Review IT service level agreement (SLA) metrics.
- ☐ Analyze downtime frequency and duration.

Explanation:

Explanation:

A service level agreement (SLA) is a written document, which officially describe the details of services, in non-technical terms, provided by the IT department (internal or external) to its customers. The aim of SLA is to maintain and improve the customer satisfaction to an agreed level.

Licensed to Berend Post berend.post@it-university.nl

Question 1272

Following a recent acquisition, an information security manager has been requested the outstanding risk reported early in the acquisition process. Which of the following would be the manager's BESTcourse of action?

- ☐ Perform a vulnerability assessment of the acquired company's infrastructure.
- ☐ Re-evaluate the risk treatment plan for the outstanding risk.
- ☒ Re-assess the outstanding risk of the acquired company.
- ☐ Add the outstanding risk to the acquiring organization's risk registry

Question 1273

Active radio frequency ID (RFID) tags are subject to which of the following exposures?

- ☐ Session hijacking
- ☒ Eavesdropping
- ☐ Malicious code
- ☐ Phishing

Explanation:

Explanation:

Like wireless devices, active RFID tags are subject to eavesdropping. They are by nature not subject to session hijacking, malicious code or phishing.

Question 1274

When building a corporate-wide business continuity plan, it is discovered there are two separate lines of business systems that could be impacted by the same threat. Which of the following is the BEST method to determine the priority of systems recovery in the event of a disaster?

- ☐ Reviewing the business plans of each department
- ☒ Evaluating the cost associated with each system's outage
- ☐ Reviewing each system's key performance indicators (KPIs)
- ☐ Comparing the recovery point objectives (RPOs)

Question 1275

Which of the following is an environmental issue caused by electric storms or noisy electric equipment and may also cause computer system to hang or crash?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☒ EMI

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

Because Unshielded Twisted Pair cables does not have shielding like shielded twisted-pair cables, UTP is susceptible to interference from external electrical sources, which could reduce the integrity of the signal. Also, to intercept transmitted data, an intruder can install a tap on the cable or monitor the radiation from the wire. Thus, UTP may not be a good choice when transmitting very sensitive data or when installed in an environment with much electromagnetic interference (EMI) or radio frequency interference (RFI). Despite its drawbacks, UTP is the most common cable type. UTP is inexpensive, can be easily bent during installation, and, in most cases, the risk from the above drawbacks is not enough to justify more expensive cables.

For your exam you should know below information about power failure

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Sags, spike and surge – Temporary and rapid decreases (sag) or increases (spike and surges) in a voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices.

Electromagnetic interference (EMI) - The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

The following were incorrect answers:

Sag – Temporarily rapid decrease in a voltage.

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

 Licensed to Berend Post berend.post@it-university.nl

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number372

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6507-6512). Acerbic Publications. Kindle Edition.

Question 1276

The BEST way to validate whether a malicious act has actually occurred in an application is to review:

- ☐ segregation of duties
- ☐ access controls
- ☒ activity logs
- ☐ change management logs

Question 1277

Business applications should be selected for disaster recovery testing on the basis of:

- ☐ the results of contingency desktop checks
- ☐ the number of failure points that are being tested
- ☒ recovery time objectives (RTOs)
- ☐ criticality to the enterprise

Question 1278

An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

- ☒ violations may not be categorized according to the organization's risk profile.
- ☐ violation reports may not be retained according to the organization's risk profile.
- ☐ violation reports may not be reviewed in a timely manner.
- ☐ a significant number of false positive violations may be reported.

Licensed to Berend Post berend.post@it-university.nl

Question 1279

Which of the following should be the PRIMARY objective of the information security incident response process?

- ☒ Minimizing negative impact to critical operations
- ☐ Communicating with internal and external parties
- ☐ Classifying incidents
- ☐ Conducting incident triage

Question 1280

To provide protection for media backup stored at an offsite location, the storage site should be:

- ☐ located on a different floor of the building.
- ☐ easily accessible by everyone.
- ☐ clearly labeled for emergency access.
- ☒ protected from unauthorized access.

Explanation:

Explanation:

The offsite storage site should always be protected against unauthorized access and have at least the same security requirements as the primary site. Choice A is incorrect because, if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.

Question 1281

An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

- ☒ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Explanation:

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need. A warm site is an offsite backup facility that is partially configured with network connections and selected peripheral equipment-such as disk and tape units, controllers and CPUs-to operate an information processing facility. A duplicate information processing facility is a dedicated, self-developed recovery site that can back up critical applications.

Licensed to Berend Post berend.post@it-university.nl

Question 1282

A recent audit has identified that security controls required by the organization's policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?

- ☐ Deny access to the application until the issue is resolved.
- ☐ Discuss the issue with data custodians to determine the reason for the exception.
- ☐ Report the issue to senior management and request funding to fix the issue.
- ☒ Discuss the issue with data owners to determine the reason for the exception.

Question 1283

Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?

- ☒ Balanced scorecards
- ☐ Benchmarking
- ☐ Maturity models
- ☐ Peer reviews

Question 1284

Which of the following concerns is BEST addressed by securing production source libraries?

- ☒ Production source and object libraries may not be synchronized.
- ☐ Unauthorized changes can be moved into production.
- ☐ Programs are not approved before production source libraries are updated.
- ☐ Changes are applied to the wrong version of production source libraries.

Question 1285

What is the first step in a business process re-engineering project?

- ☐ Identifying current business processes
- ☐ Forming a BPR steering committee
- ☒ Defining the scope of areas to be reviewed
- ☐ Reviewing the organizational strategic plan

Explanation:

Explanation: Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

Licensed to Berend Post berend.post@it-university.nl

Question 1286

Which of the following is not a good tactic to use against hackers?

- ☐ Enticement
- ☒ Entrapment

Explanation:

Explanation:

Enticement occurs after somebody has gained unlawful access to a system and then subsequently lured to a honey pot. Entrapment encourages the commitment of unlawful access. The latter is not a good tactic to use as it involves encouraging someone to commit a crime.

Question 1287

When are benchmarking partners identified within the benchmarking process?

- ☐ In the design stage
- ☐ In the testing stage
- ☒ In the research stage
- ☐ In the development stage

Explanation:

Explanation:

Benchmarking partners are identified in the research stage of the benchmarking process.

Question 1288

The IS auditor's PRIMARY role in control self-assessment (CSA) is to:

- ☐ evaluate the controls.
- ☐ facilitate the process.
- ☒ identify weaknesses.
- ☐ draw up an action plan.

Question 1289

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- ☐ Test data
- ☒ Generalized audit software
- ☐ Integrated test facility
- ☐ Embedded audit module

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. An IS auditor, using generalized audit software, could design appropriate tests to recompute the payroll, thereby determining if there were overpayments and to whom they were made. Test data would test for the existence of controls that might prevent overpayments, but it would not detect specific, previous miscalculations. Neither an integrated test facility nor an embedded audit module would detect errors for a previous period.

Question 1290

Outsourcing the development of business systems is MOST likely to result in the loss of:

- ☒ control over strategic direction.
- ☐ accountability for end products.
- ☐ in-house competencies.
- ☐ responsibility for IT security.

Question 1291

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- ☒ vulnerabilities.
- ☐ threats.
- ☐ probabilities.
- ☐ impacts.

Explanation:

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

Question 1292

An audit of the quality management system (QMS) begins with an evaluation of the:

- ☒ organization's QMS policy
- ☐ sequence and interaction of QMS processes
- ☐ QMS processes and their application
- ☐ QMS document control procedures

Licensed to Berend Post berend.post@it-university.nl

Question 1293

A warehouse employee of a retail company has been able to conceal the theft of inventory items by entering adjustments of either damaged or lost stock items to the inventory system. Which control would have BEST prevented this type of fraud in a retail environment?

- ☐ An edit check for the validity of the inventory transaction
- ☒ Separate authorization for input of transactions
- ☐ Unscheduled audits of lost stock lines
- ☐ Statistical sampling of adjustment transactions

Question 1294

An IS auditor begins an assignment and identifies audit components for which the auditor is not qualified to assess. Which of the following is the BEST course of action?

- ☒ Notify audit management for a decision on how to proceed.
- ☐ Complete the audit and give full disclosure in the final audit report.
- ☐ Complete the work assignment to the best of the auditor's ability.
- ☐ Exclude the related tests from the audit plan and continue the assignment.

Question 1295

Which of the following statement correctly describes difference between packet filtering firewall and stateful inspection firewall?

- ☒ Packet filtering firewall do not maintain client session whereas Stateful firewall maintains client session.
- ☐ Packet filtering firewall and Stateful firewall both maintain session of client.
- ☐ Packet filtering firewall is a second generation firewall whereas Stateful is a first generation of firewall.
- ☐ Packet filtering firewall and Stateful firewall do not maintain any session of client.

Explanation:

Packet Filtering Firewall

Also Known as First Generation Firewall

Do not maintain client session

The advantage of this type of firewall are simplicity and generally stable performance since the filtering rules are performed at the network layer.

Its simplicity is also disadvantage, because it is vulnerable to attack from improperly configured filters and attack tunneled over permitted services.

Some of the more common attack on packet filtering are IP Spoofing, Source Routing specification, Miniature fragment attack.

Licensed to Berend Post berend.post@it-university.nl

Stateful Inspection Firewall

A stateful inspection firewall keep track of the destination IP address of each packet that leaves the organization's internal network.

The session tracking is done by mapping the source IP address of incoming packet with the list of destination IP addresses that is maintained and updated

This approach prevent any attack initiated and originated by outsider.

The disadvantage includes stateful inspection firewall can be relatively complex to administer as compare to other firewall.

The following were incorrect answers:

All other choices presented were incorrect answers because they all had the proper definition.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 345 and 346

Question 1296

What is used as a control to detect loss, corruption, or duplication of data?

- ☐ Redundancy check
- ☐ Reasonableness check
- ☒ Hash totals
- ☐ Accuracy check

Explanation:

Explanation:

Hash totals are used as a control to detect loss, corruption, or duplication of data.

Question 1297

Why is a clause for requiring source code escrow in an application vendor agreement important?

- ☐ To segregate systems development and live environments
- ☐ To protect the organization from copyright disputes
- ☐ To ensure that sufficient code is available when needed
- ☒ To ensure that the source code remains available even if the application vendor goes out of business

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A clause for requiring source code escrow in an application vendor agreement is important to ensure that the source code remains available even if the application vendor goes out of business.

Question 1298

During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

- ☐ increased maintenance.
- ☐ improper documentation of testing.
- ☒ inadequate functional testing.
- ☐ delays in problem resolution.

Explanation:

Explanation:

The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B and D are not as important.

Question 1299

The goal of an information system is to achieve integrity, authenticity and non-repudiation of information's sent across the network. Which of the following statement correctly describe the steps to address all three?

- ☐ Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message.
- ☐ Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key.
- ☐ Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key.
- ☒ Encrypt message digest using sender's private key and then send the encrypted digest to the receiver along with original message. Receiver can decrypt the same using sender's public key.

Explanation:

The digital signature is used to achieve integrity, authenticity and non-repudiation. In a digital signature, the sender's private key is used to encrypt the message digest of the message. Encrypting the message digest is the act of Signing the message. The receiver will use the matching public key of the sender to decrypt the Digital Signature using the sender's public key.

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and

Licensed to Berend Post berend.post@it-university.nl

possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures cannot be forged by someone else who does not possess the private key, it can also be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real and has not been modified since the day it was issued.

How Digital Signature Works

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

You copy-and-paste the contract (it's a short one!) into an e-mail note.

Using special software, you obtain a message hash (mathematical summary) of the contract.

You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.

The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

To make sure it's intact and from you, your lawyer makes a hash of the received message.

Your lawyer then uses your public key to decrypt the message hash or summary.

If the hashes match, the received message is valid.

Below are some common reasons for applying a digital signature to communications:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. The importance of high assurance in the sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office

 Licensed to Berend Post berend.post@it-university.nl

requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a serious mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it.(Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after the signature has been applied would invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that authentication, non-repudiation, and other properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". This is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen.

Tip for the exam

Digital Signature does not provide confidentiality. It provides only authenticity and integrity. The sender's private key is used to encrypt the message digest to calculate the digital signature

Encryption provides only confidentiality. The receiver's public key or symmetric key is used for encryption

The following were incorrect answers:

Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message - Symmetric key encryption does not provide non-repudiation as symmetric key is shared between users

Licensed to Berend Post berend.post@it-university.nl

Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key - Receiver's public key is known to everyone. This will not address non-repudiation

Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key -The sender public key is known to everyone. If sender's key is used for encryption, then sender's private key is required to decrypt data. The receiver will not be able to decrypt the digest as receiver will not have sender's private key.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 331

http://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg

http://en.wikipedia.org/wiki/Digital_signature

http://searchsecurity.techtarget.com/definition/digital-signature

Question 1300

Which of the following measures can protect systems files and data, respectively?

- ☒ User account access controls and cryptography
- ☐ User account access controls and firewall
- ☐ User account access controls and IPS
- ☐ IDS and cryptography
- ☐ Firewall and cryptography
- ☐ None of the choices.

Explanation:

Explanation:

User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

Licensed to Berend Post berend.post@it-university.nl

Question 1301

Which of the following is the GREATEST risk posed by denial-of-service attacks?

- ☐ Confidential information leakage
- ☐ Loss of integrity and corruption of databases
- ☒ Loss of reputation and business
- ☐ Unauthorized access to the systems

Question 1302

An IS auditor who was involved in designing an organization's business continuity plan(BCP) has been assigned to audit the plan. The IS auditor should:

- ☐ decline the assignment.
- ☐ inform management of the possible conflict of interest after completing the audit assignment.
- ☐ inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
- ☒ communicate the possibility of conflict of interest to management prior to starting the assignment.

Explanation:

Explanation:

Communicating the possibility of a conflict of interest to management prior to starting the assignment is the correct answer. A possible conflict of interest, likely to affect the auditor's independence, should be brought to the attention of management prior to starting the assignment. Declining the assignment is not the correct answer because the assignment could be accepted after obtaining management approval. Informing management of the possible conflict of interest after completion of the audit assignment is not correct because approval should be obtained prior to commencement and not after the completion of the assignment. Informing the business continuity planning (BCP) team of the possible conflict of interest prior to starting of the assignment is not the correct answer since the BCP team would not have the authority to decide on this issue.

Question 1303

An organization's IS audit charter should specify the:

- ☐ short- and long-term plans for IS audit engagements
- ☐ objectives and scope of IS audit engagements.
- ☐ detailed training plan for the IS audit staff.
- ☒ role of the IS audit function.

Explanation:

Explanation:

An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved

Licensed to Berend Post berend.post@it-university.nl

by the highest level of management and, if available, by the audit committee. Short- term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

Question 1304

Which of the following control make sure that input data comply with predefined criteria maintained in computerized table of possible values?

- ☐ Range Check
- ☒ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Explanation:

In table lookups input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check - Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Validity Check - Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an

Licensed to Berend Post berend.post@it-university.nl

order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification -The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check- new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Range Check -Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 215

Question 1305

For application acquisitions with significant impacts, participation of your IS audit team should be encouraged:

- ☒ early in the due diligence stage.
- ☐ at the testing stage.
- ☐ at the final approval stage.
- ☐ at the budget preparation stage.
- ☐ None of the choices.

Explanation:

Explanation:

For acquisitions with significant IT impacts, participation of IS audit is often necessary early in the due diligence stage as defined in the audit policy.

Question 1306

Information security awareness programs are MOST effective when they are:

- ☒ customized for each target audience
- ☐ conducted at employee orientation
- ☐ reinforced by computer-based training
- ☐ sponsored by senior management

Licensed to Berend Post berend.post@it-university.nl

Question 1307

To verify that the correct version of a data file was used for a production run, an IS auditor should review:

- ☐ operator problem reports.
- ☐ operator work schedules.
- ☒ system logs.
- ☐ output distribution reports.

Explanation:

Explanation:

System logs are automated reports which identify most of the activities performed on the computer. Programs that analyze the system log have been developed to report on specifically defined items. The auditor can then carry out tests to ensure that the correct file version was used for a production run. Operator problem reports are used by operators to log computer operation problems. Operator work schedules are maintained to assist in human resources planning.

Output distribution reports identify all application reports generated and their distribution.

Question 1308

Which of the following BEST enables timely detection of changes in the IT environment to support informed decision making by management?

- ☒ Continuous monitoring
- ☐ Sampling checks on high-risk areas
- ☐ Change management reports
- ☐ Established key risk indicators (KRIs)

Question 1309

When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

- ☐ Passwords are not shared.
- ☒ Password files are not encrypted.
- ☐ Redundant logon IDs are deleted.
- ☐ The allocation of logon IDs is controlled.

Explanation:

Explanation:

When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon IDs and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

Licensed to Berend Post berend.post@it-university.nl

Question 1310

Which of the following cryptography is based on practical application of the characteristics of the smallest “grains” of light, the photon, the physical laws governing their generation and propagation and detection?

- ☒ Quantum Cryptography
- ☐ Elliptical Curve Cryptography (ECC)
- ☐ Symmetric Key Cryptography
- ☐ Asymmetric Key Cryptography

Explanation:

Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection.

Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection.

Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

The following were incorrect answers: Elliptic Key Cryptography(ECC) - A variant and more efficient form of a public key cryptography (how to manage more security out of minimum resources) gaining prominence is the ECC. ECC works well on a network computer requires strong cryptography but have some limitation such as bandwidth and processing power. This is even more important with devices such as smart cards, wireless phones and other mobile devices. It is believed that ECC demands less computational power and, therefore offers more security per bit. For example, an ECC with a 160-bit key offer the same security as an RSA based system with a 1024-bit key.

Symmetric Encryption- Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number of places in the alphabet. As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message.

 Licensed to Berend Post berend.post@it-university.nl

Asymmetric encryption -In which there are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.

Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key.

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 349 and 350

http://support.microsoft.com/kb/246071

Question 1311

The MAIN purpose for periodically testing offsite facilities is to:

- ☐ protect the integrity of the data in the database.
- ☐ eliminate the need to develop detailed contingency plans.
- ☒ ensure the continued compatibility of the contingency facilities.
- ☐ ensure that program and system documentation remains current.

Explanation:

Explanation:

The main purpose of offsite hardware testing is to ensure the continued compatibility of the contingency facilities. Specific software tools are available to protect the ongoing integrity of the database. Contingency plans should not be eliminated and program and system documentation should be reviewed continuously for currency.

Licensed to Berend Post berend.post@it-university.nl

Question 1312

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

- ☒ Piggybacking
- ☐ Shoulder surfing
- ☐ Dumpster diving
- ☐ Impersonation

Explanation:

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have their badge read at every controlled door no unauthorized person could enter the sensitive area. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

Question 1313

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

- ☐ meets or exceeds industry security standards.
- ☒ agrees to be subject to external security reviews.
- ☐ has a good market reputation for service and experience.
- ☐ complies with security policies of the organization.

Explanation:

Explanation:

It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify or prove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

Licensed to Berend Post berend.post@it-university.nl

Question 1314

A live test of a mutual agreement for IT system recovery has been carried out, including a four- hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

- ☒ system and the IT operations team can sustain operations in the emergency environment.
- ☐ resources and the environment could sustain the transaction load.
- ☐ connectivity to the applications at the remote site meets response time requirements.
- ☐ workflow of actual business operations can use the emergency system in case of a disaster.

Explanation:

Explanation:

The applications have been intensively operated, therefore choices B, C and D have been actually tested, but the capability of the system and the IT operations team to sustain and support this environment (ancillary operations, batch closing, error corrections, output distribution, etc.) is only partially tested.

Question 1315

Which of the following BEST ensures that effective change management is in place in an IS environment?

- ☒ User authorization procedures for application access are well established.
- ☐ User-prepared detailed test criteria for acceptance testing of the software.
- ☐ Adequate testing was carried out by the development team.
- ☐ Access to production source and object programs is well controlled.

Question 1316

An IS auditor concludes that a local area network's (LAN's) access security is satisfactory. In reviewing the work, the audit manager should:

- ☐ re-perform some steps of the audit to verify the quality of the work.
- ☒ verify that the elements of an agreed-upon audit plan have been addressed.
- ☐ verify user management's agreement with the findings.
- ☐ assess whether the auditor had the appropriate skills to perform the work.

Licensed to Berend Post berend.post@it-university.nl

Question 1317

The PRIMARY objective of value delivery in reference to IT governance is to:

- ☐ increase efficiency
- ☐ promote best practices
- ☒ optimize investments
- ☐ ensure compliance

Question 1318

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

- ☒ payroll reports should be compared to input forms.
- ☐ gross payroll should be recalculated manually.
- ☐ checks (cheques) should be compared to input forms.
- ☐ checks (cheques) should be reconciled with output reports.

Explanation:

Explanation:

The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques)have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

Question 1319

Before a failover test of a critical business application is performed, it is MOST important for the information security manager to:

- ☐ obtain a signed risk acceptation from the recovery team
- ☒ obtain senior management's approval
- ☐ inform the users that the test is taking place
- ☐ verify that the information assets have been classified properly

Licensed to Berend Post berend.post@it-university.nl

Question 1320

Hamid needs to shift users from using the application from the existing (Old) system to the replacing (new) system. His manager Lily has suggested he uses an approach in which the newer system is changed over from the older system on a cutoff date and time and the older system is discontinued once the changeover to the new system takes place. Which of the following changeover approach is suggested by Lily?

- ☐ Parallel changeover
- ☐ Phased changeover
- ☒ Abrupt changeover
- ☐ Pilot changeover

Explanation:

In the abrupt changeover approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system.

Changeover to newer system involves four major steps or activities

Conversion of files and programs; test running on test bed

Installation of new hardware, operating system, application system and the migrated data.

Training employees or user in groups

Scheduling operations and test running for go-live or changeover

Some of the risk areas related to changeover includes:

Asset safeguarding

Data integrity

System effectiveness

Change management challenges

Duplicate or missing records

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Parallel changeover – This technique includes running the old system, then running both the old and new systems in parallel and finally full changing over to the new system after gaining confidence in the working of new system.

Phased Changeover -In this approach the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.

Pilot changeover – Not a valid changeover type.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 172

Question 1321

Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

- ☐ The disaster levels are based on scopes of damaged functions, but not on duration.
- ☐ The difference between low-level disaster and software incidents is not clear.
- ☐ The overall BCP is documented, but detailed recovery steps are not specified.
- ☒ The responsibility for declaring a disaster is not identified.

Explanation:

Explanation:

If nobody declares the disaster, the response and recovery plan would not be invoked, making all other concerns mute. Although failure to consider duration could be a problem, it is not as significant as scope, and neither is as critical as the need to have someone invoke the plan. The difference between incidents and low-level disasters is always unclear and frequently revolves around the amount of time required to correct the damage. The lack of detailed steps should be documented, but their absence does not mean a lack of recovery, if in fact someone has invoked the plan.

Question 1322

Which of the following BEST indicates a need to review an organization's information security policy?

- ☐ Completion of annual IT risk assessment
- ☒ Increasing complexity of business transactions
- ☐ Increasing exceptions approved by management
- ☐ High number of low-risk findings in the audit report

Licensed to Berend Post berend.post@it-university.nl

Question 1323

Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

- ☒ Develop a baseline and monitor system usage.
- ☐ Define alternate processing procedures.
- ☐ Prepare the maintenance manual.
- ☐ implement the changes users have suggested.

Explanation:

Explanation:

An IS auditor should recommend the development of a performance baseline and monitor the system's performance, against the baseline, to develop empirical data upon which decisions for modifying the system can be made. Alternate processing procedures and a maintenance manual will not alter a system's performance. Implementing changes without knowledge of the cause(s) for the perceived poor performance may not result in a more efficient system.

Question 1324

During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:

- ☐ assessment of the situation may be delayed.
- ☒ execution of the disaster recovery plan could be impacted.
- ☐ notification of the teams might not occur.
- ☐ potential crisis recognition might be ineffective.

Explanation:

Explanation: Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster. Once a potential crisis is recognized, the teams responsible for crisis management need to be notified. Delaying this step until a disaster has been declared would negate the effect of having response teams. Potential crisis recognition is the first step in responding to a disaster.

Question 1325

Which of the following will identify a deviation in the information security management process from generally accepted standards of good practices?

- ☒ Gap analysis
- ☐ Risk assessment
- ☐ Business impact analysis (BIA)
- ☐ Penetration testing

Licensed to Berend Post berend.post@it-university.nl

Question 1326

Inadequate programming and coding practices introduce the risk of:

- ☐ phishing.
- ☒ buffer overflow exploitation.
- ☐ SYN flood.
- ☐ brute force attacks.

Explanation:

Explanation:

Buffer overflow exploitation may occur when programs do not check the length of the data that are input into a program. An attacker can send data that exceed the length of a buffer and override part of the program with malicious code. The countermeasure is proper programming and good coding practices. Phishing, SYN flood and brute force attacks happen independently of programming and coding practices.

Question 1327

Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?

- ☐ Vulnerability assessment results
- ☐ Application security policy
- ☒ A business case
- ☐ Internal audit reports

Question 1328

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- ☒ Firewalls
- ☐ Routers
- ☐ Layer 2 switches
- ☐ VLANs

Explanation:

Explanation:

Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool. Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

Licensed to Berend Post berend.post@it-university.nl

Question 1329

An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

- ☐ a backup server be available to run ETCS operations with up-to-date data.
- ☐ a backup server be loaded with all the relevant software and data.
- ☐ the systems staff of the organization be trained to handle any event.
- ☒ source code of the ETCS application be placed in escrow.

Explanation:

Explanation:

Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business. Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

Question 1330

Which of the following sampling methods is MOST useful when testing for compliance?

- ☒ Attribute sampling
- ☐ Variable sampling
- ☐ Stratified mean per unit
- ☐ Difference estimation

Explanation:

Explanation:

Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testing to confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

Question 1331

Which of the following BEST facilitates compliance with requirements mandating the security of confidential data?

- ☐ Classification of data
- ☐ Security awareness training
- ☒ Encryption of external data transmissions
- ☐ Standardized escalation protocols for breaches

Licensed to Berend Post berend.post@it-university.nl

Question 1332

An IS auditor is conducting a review of a healthcare organization's IT policies for handling medical records. Which of the following is MOST important to verify?

- ☐ A documented policy approval process is in place
- ☐ Policy writing standards are consistent
- ☒ The policies comply with regulatory requirements
- ☐ IT personnel receive ongoing policy training

Question 1333

The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

- ☒ searches and checks the infrastructure to detect vulnerabilities, whereas penetration testing intends to exploit the vulnerabilities to probe the damage that could result from the vulnerabilities.
- ☐ and penetration tests are different names for the same activity.
- ☐ is executed by automated tools, whereas penetration testing is a totally manual process.
- ☐ is executed by commercial tools, whereas penetration testing is executed by public processes.

Explanation:

Explanation:

The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed; its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same; they have different approaches. Vulnerability assessments and penetration testing can be executed by automated or manual tools or processes and can be executed by commercial or free tools.

Question 1334

"Nowadays, computer security comprises mainly "preventive"" measures."

- ☒ True
- ☐ True only for trusted networks
- ☐ True only for untrusted networks
- ☐ False
- ☐ None of the choices.

Explanation:

Explanation:

"Nowadays, computer security comprises mainly ""preventive"" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network

Licensed to Berend Post berend.post@it-university.nl

and another network and is normally implemented as software running on the machine or as physical integrated hardware."

Question 1335

Invoking a business continuity plan (BCP) is demonstrating which type of control?

- ☐ Corrective
- ☒ Preventive
- ☐ Detective
- ☐ Directive

Question 1336

From a control perspective, the PRIMARY objective of classifying information assets is to:

- ☒ establish guidelines for the level of access controls that should be assigned.
- ☐ ensure access controls are assigned to all information assets.
- ☐ assist management and auditors in risk assessment.
- ☐ identify which assets need to be insured against losses.

Explanation:

Explanation:

Information has varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources, management can establish guidelines for the level of access controls that should be assigned. End user management and the security administrator will use these classifications in their risk assessment process to assign a given class to each asset.

Question 1337

Which of the following should be the MOST important consideration when establishing data classification standards?

- ☐ An education campaign is established upon rollout.
- ☐ Reporting metrics are established.
- ☒ Management supports the newly developed standards.
- ☐ The standards comply with relevant regulations.

Licensed to Berend Post berend.post@it-university.nl

Question 1338

The ultimate purpose of IT governance is to:

- ☒ encourage optimal use of IT.
- ☐ reduce IT costs.
- ☐ decentralize IT resources across the organization.
- ☐ centralize control of IT.

Explanation:

Explanation:

IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

Question 1339

At the completion of a system development project, a post project review should include which of the following?

- ☐ Assessing risks that may lead to downtime after the production release
- ☒ Identifying lessons learned that may be applicable to future projects
- ☐ Verifying the controls in the delivered system are working
- ☐ Ensuring that test data are deleted

Explanation:

Explanation:

A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the post implementation review. Test data should be retained for future regression testing.

Question 1340

Which of the following could lead to an unintentional loss of confidentiality?

- ☒ Lack of employee awareness of a company's information security policy
- ☐ Failure to comply with a company's information security policy
- ☐ A momentary lapse of reason
- ☐ Lack of security policy enforcement procedures

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality.

Question 1341

During a review of the IT strategic plan, an IS auditor finds several IT initiatives focused on delivering new systems and technology are not aligned with the organization's strategy. Witch of the following would be the IS auditor's BEST recommendation?

- ☐ Reassess the return on investment for the IT initiatives
- ☐ Modify IT initiatives that do not map to business strategies
- ☐ Utilize a balanced scorecard to align IT initiatives to business strategies
- ☒ Reassess IT initiatives that do not map business strategies

Question 1342

What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?

- ☐ Obtain senior management commitment.
- ☒ Test incident response procedures regularly.
- ☐ Communicate incident response procedures to staff.
- ☐ Establish and measure key performance indicators (KPIs).

Question 1343

An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

- ☐ Controls the proliferation of multiple versions of programs
- ☒ Expands the programming resources and aids available
- ☐ Increases program and processing integrity
- ☐ Prevents valid changes from being overwritten by other changes

Explanation:

Explanation:

A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

Licensed to Berend Post berend.post@it-university.nl

Question 1344

The effectiveness of an information security governance framework will BEST be enhanced if:

- ☐ consultants review the information security governance framework
- ☒ a culture of legal and regulatory compliance is promoted by management
- ☐ IS auditors are empowered to evaluate governance activities
- ☐ risk management is built into operational and strategic activities

Question 1345

Which of the following should the IS auditor do FIRST to ensure data transfer integrity for Internet of Things (IoT) devices?

- ☐ Verify access control lists to the database where collected data is stored.
- ☐ Confirm that acceptable limits of data bandwidth are defined for each device.
- ☐ Ensure that message queue telemetry transport (MQTT) is used.
- ☒ Determine how devices are connected to the local network.

Question 1346

A validated patch to address a new vulnerability that may affect a mission-critical server has been released. What should be done immediately?

- ☐ Add mitigating controls.
- ☐ Check the server's security and install the patch.
- ☒ Conduct an impact analysis.
- ☐ Take the server off-line and install the patch.

Question 1347

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

- ☐ Security administrator
- ☐ Systems auditor
- ☒ Board of directors
- ☐ Financial auditor

Explanation:

Explanation:

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

Licensed to Berend Post berend.post@it-university.nl

Question 1348

In a security server audit, focus should be placed on (Choose two.):

- ☒ proper segregation of duties
- ☐ adequate user training
- ☒ continuous and accurate audit trail
- ☐ proper application licensing
- ☐ system stability
- ☐ performance and controls of the system
- ☐ None of the choices.

Question 1349

Which of the following comparisons are used for identification and authentication in a biometric system?

- ☐ One-to-many for identification and authentication
- ☐ One-to-one for identification and authentication
- ☒ One-to-many for identification and one-to-one for authentication
- ☐ One-to-one for identification and one-to-many for authentication

Explanation:

In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be"

In verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution and processing of biometrics data encompassing:

Data integrity, authenticity and non-repudiation

Management of biometric data across its life cycle – compromised of the enrollment, transmission and storage, verification, identification, and termination process

Usage of biometric technology, including one-to-one and one-to-many matching, for identification and authentication

Licensed to Berend Post berend.post@it-university.nl

Application of biometric technology for internal and external, as well as logical and physical access control

Encapsulation of biometric data

Security of the physical hardware used throughout the biometric data life cycle

Techniques for integrity and privacy protection of biometric data.

The following were incorrect answers:

All other choices presented were incorrectly describing identification and authentication mapping.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 331

http://en.wikipedia.org/wiki/Biometrics

Question 1350

Which of the following is an advantage of an integrated test facility (ITF)?

- ☐ It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.
- ☒ Periodic testing does not require separate test processes.
- ☐ It validates application systems and tests the ongoing operation of the system.
- ☐ The need to prepare test data is eliminated.

Explanation:

Explanation: An integrated test facility creates a factitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

Licensed to Berend Post berend.post@it-university.nl

Question 1351

Which of the following audit risk is related to material errors or misstatements that have occurred that will not be detected by an IS auditor?

- ☐ Inherent Risk
- ☐ Control Risk
- ☒ Detection Risk
- ☐ Overall Audit Risk

Explanation:

Explanation:

The risk that material errors or misstatements that have occurred will not be detected by an IS auditor. Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements. An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions. Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

For your exam you should know below information about audit risk:

Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR), and can be calculated thus:

AR = IR • CR • DR

Inherent Risk

Auditors must determine risks when working with clients. One type of risk to be aware of is inherent risk. While assessing this level of risk, you ignore whether the client has internal controls in place (such as a secondary review of financial statements) in order to help mitigate the inherent risk. You consider the strength of the internal controls when assessing the client's control risk. Your job when assessing inherent risk is to evaluate how susceptible the financial statement assertions are to material misstatement given the nature of the client's business. A few key factors can increase inherent risk.

Environment and external factors: Here are some examples of environment and external factors that can lead to high inherent risk:

Licensed to Berend Post berend.post@it-university.nl

Rapid change: A business whose inventory becomes obsolete quickly experiences high inherent risk.

Expiring patents: Any business in the pharmaceutical industry also has inherently risky environment and external factors. Drug patents eventually expire, which means the company faces competition from other manufacturers marketing the same drug under a generic label.

State of the economy: The general level of economic growth is another external factor affecting all businesses.

Availability of financing: Another external factor is interest rates and the associated availability of financing. If your client is having problems meeting its short-term cash payments, available loans with low interest rates may mean the difference between your client staying in business or having to close its doors.

Prior-period misstatements: If a company has made mistakes in prior years that weren't material (meaning they weren't significant enough to have to change), those errors still exist in the financial statements. You have to aggregate prior-period misstatements with current year misstatements to see if you need to ask the client to adjust the account for the total misstatement.

You may think an understatement in one year compensates for an overstatement in another year. In auditing, this assumption isn't true. Say you work a cash register and one night the register comes up $20 short. The next week, you somehow came up $20 over my draw count. The $20 differences are added together to represent the total amount of your mistakes which is $40 and not zero. Zero would indicate no mistakes at all had occurred.

Susceptibility to theft or fraud: If a certain asset is susceptible to theft or fraud, the account or balance level may be considered inherently risky. For example, if a client has a lot of customers who pay in cash, the balance sheet cash account is going to have risk associated with theft or fraud because of the fact that cash is more easily diverted than customer checks or credit card payments.

Looking at industry statistics relating to inventory theft, you may also decide to consider the inventory account as inherently risky. Small inventory items can further increase the risk of this account valuation being incorrect because those items are easier to conceal (and therefore easier to steal).

Control Risk

Control risk has been defined under International Standards of Auditing (ISAs) as following:

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control.

Licensed to Berend Post berend.post@it-university.nl

In simple words control risk is the probability that a material misstatement exists in an assertion because that misstatement was not either prevented from entering entity's financial information or it was not detected and corrected by the internal control system of the entity.

It is the responsibility of the management and those charged with governance to implement internal control system and maintain it appropriately which includes managing control risk.

There can be many reasons for control risk to arise and why it cannot be eliminated absolutely. But some of them are as follows:

Cost-benefit constraints

Circumvention of controls

Inappropriate design of controls

Inappropriate application of controls

Lack of control environment and accountability

Novel situations

Outdated controls

Inappropriate segregation of duties

Detection Risk

Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements.

An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions.

Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

Inherent Risk - It is the risk level or exposure of a process or entity to be audited without taking into account the control that management has implemented.

Control Risk - The risk that material error exist that would not be prevented or detected on timely basis by the system of internal controls.

Overall audit risk - The probability that information or financial report may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under security so the overall audit risk is at sufficiently low level at the completion of the examination.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 50

http://en.wikipedia.org/wiki/Audit_risk

http://www.dummies.com/how-to/content/how-to-assess-inherent-risk-in-an-audit.html

http://pakaccountants.com/what-is-control-risk/

http://accounting-simplified.com/audit/risk-assessment/audit-risk.html

Question 1352

In an online banking application, which of the following would BEST protect against identity theft?

- ☐ Encryption of personal password
- ☐ Restricting the user to a specific terminal
- ☒ Two-factor authentication
- ☐ Periodic review of access logs

Explanation:

Explanation:

Two-factor authentication requires two independent methods for establishing identity and privileges. Factors include something you know, such as a password; something you have, such as a token; and something you are, which is biometric. Requiring two of these factors makes identity theft more difficult. A password could be guessed or broken. Restricting the user to a specific terminal is not a practical alternative for an online application. Periodic review of access logs is a detective control and does not protect against identity theft.

Licensed to Berend Post berend.post@it-university.nl

Question 1353

Which of the following risk handling technique involves the practice of being proactive so that the risk in question is not realized?

- ☐ Risk Mitigation
- ☐ Risk Acceptance
- ☒ Risk Avoidance
- ☐ Risk transfer

Explanation:

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized.

For your exam you should know below information about risk assessment and treatment:

A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. A risk assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security controls, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

Identify assets and their value to the organization.

Identify vulnerabilities and threats.

Quantify the probability and business impact of these potential threats.

Provide an economic balance between the impact of the threat and the cost

of the countermeasure.

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion

Licensed to Berend Post berend.post@it-university.nl

detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance.

It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before committing to owning, insuring, and driving a motor vehicle.

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if, indeed, the company has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could have a catastrophic effect on the company's ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

Licensed to Berend Post berend.post@it-university.nl

For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase of new hardware, software, and office equipment, while transference of the risk to an insurance company would require premium payments. The

executive then further notes that minimal impact to the organization would occur if any of the reported low-level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to forgo the costs and accept the risk. In the young driver example, risk acceptance could be based on the observation that the youngster has demonstrated the responsibility and maturity to warrant the parent's trust in his or her judgment.

The following answers are incorrect:

Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

Risk Acceptance - Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

Risk Mitigation -Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 51

and

Official ISC2 guide to CISSP CBK 3rd edition page number 534-536

Licensed to Berend Post berend.post@it-university.nl

Question 1354

Before implementing an IT balanced scorecard, an organization must:

- ☐ deliver effective and efficient services.
- ☒ define key performance indicators.
- ☐ provide business value to IT projects.
- ☐ control IT expenses.

Explanation:

Explanation:

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

Question 1355

An auditor notes the administrator user ID is shared among three financial managers to perform month-end updates. Which of the following is the BEST recommendation to ensure the administrator ID in the financial system is controlled effectively?

- ☒ Implement use of individual software tokens
- ☐ Conduct employee awareness training
- ☐ Institute user ID logging and monitoring
- ☐ Ensure data in the financial systems has been classified

Question 1356

A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration in establishing a contingency plan and an alternate processing site?

- ☒ The alternative site does not reside on the same fault no matter how far the distance apart.
- ☐ The contingency plan for high priority applications does not involve a shared cold site.
- ☐ The alternative site is a hot site with equipment ready to resume processing immediately.
- ☐ The contingency plan provides for backup tapes to be taken to the alternative site.

Licensed to Berend Post berend.post@it-university.nl

Question 1357

Who provides the funding to the project and works closely with the project manager to define critical success factor (CSF)?

- ☒ Project Sponsor
- ☐ Security Officer
- ☐ User Management
- ☐ Senior Management

Explanation:

Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

For the CISA exam you should know the information below about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management -Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?

How reliable is the software?

How effective is the software?

Is the software easy to use?

How easy is to transfer or adapt old data from preexisting software to this environment?

Is it possible to add new functions?

Does it meet regulatory requirement?

Project Steering Committee -Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised

Licensed to Berend Post berend.post@it-university.nl

of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

System Development Management -Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager -Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor - Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team -Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team -Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

User Management -Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 150

Question 1358

An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

- ☒ reduces the risk of unauthorized access to the network.
- ☐ is not suitable for small networks.
- ☐ automatically provides an IP address to anyone.
- ☐ increases the risks associated with Wireless Encryption Protocol (WEP).

Explanation:

Explanation:

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to anyone connected to the network. With DHCP disabled, static IP addresses must be used and represent less risk due to the potential for address contention between an unauthorized device and existing devices on the network. Choice B is incorrect because DHCP is suitable for small networks.

Choice C is incorrect because DHCP does not provide IP addresses when disabled. Choice D is incorrect because disabling of the DHCP makes it more difficult to exploit the well-known weaknesses in WEP.

Licensed to Berend Post berend.post@it-university.nl

Question 1359

To preserve chain of custody following an internal server compromise, which of the following should be the FIRST step?

- ☒ Take a system image including memory dump
- ☐ Safely shut down the server
- ☐ Replicate the attack using the remaining evidence
- ☐ Trace the attacking route

Question 1360

Which of the following would BEST indicate the effectiveness of a security awareness training program?

- ☐ Increased number of employees completing training
- ☐ Employee satisfaction with training
- ☐ Reduced unintentional violations
- ☒ Results of third-party social engineering tests.

Question 1361

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
- ☐ The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
- ☒ Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
- ☐ Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Explanation:

Explanation:

To ensure authenticity and confidentiality, a message must be encrypted twice: first with the sender's private key, and then with the receiver's public key. The receiver can decrypt the message, thus ensuring confidentiality of the message. Thereafter, the decrypted message can be decrypted with the public key of the sender, ensuring authenticity of the message. Encrypting the message with the sender's private key enables anyone to decrypt it.

Licensed to Berend Post berend.post@it-university.nl

Question 1362

Which of the following attacks could capture network user passwords?

- ☐ Data diddling
- ☒ Sniffing
- ☐ IP Spoofing
- ☐ Surfing

Explanation:

A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.

Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap—a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therefore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:

Data did dlinginvolves changing data before, as it is entered into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Licensed to Berend Post berend.post@it-university.nl

Surfing would refer to the surf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

The following reference(s) were/was used to create this question:

CISA Review manual 2014 Page number 321

Official ISC2 Guide to the CISSP 3rd edition Page Number 153

Question 1363

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

- ☒ Cold site
- ☐ Alternate site
- ☐ Hot site
- ☐ Warm site

Explanation:

Explanation:

Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

Question 1364

When using a digital signature, the message digest is computed:

- ☐ only by the sender.
- ☐ only by the receiver.
- ☒ by both the sender and the receiver.
- ☐ by the certificate authority (CA).

Explanation:

Explanation:

A digital signature is an electronic identification of a person or entity. It is created by using asymmetric encryption. To verify integrity of data, the sender uses a cryptographic hashing algorithm against the entire message to create a message digest to be sent along with the message. Upon receipt of the message, the receiver will recompute the hash using the same algorithm and compare results with what was sent to ensure the integrity of the message.

Licensed to Berend Post berend.post@it-university.nl

Question 1365

To effectively classify data, which of the following MUST be determined?

- ☐ Data controls
- ☒ Data ownership
- ☐ Data users
- ☐ Data volume

Question 1366

A malicious code that changes itself with each file it infects is called a:

- ☐ logic bomb.
- ☐ stealth virus.
- ☐ trojan horse.
- ☒ polymorphic virus.

Explanation:

Explanation:

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

Question 1367

Which of the following would provide the BEST justification for a new information security investment?

- ☐ Defined key performance indicators (KPIs)
- ☐ Projected reduction in risk
- ☒ Results of a comprehensive threat analysis
- ☐ Senior management involvement in project prioritization

Question 1368

Which of the following PBX feature provides the possibility to break into a busy line to inform another user of an important message?

- ☐ Account Codes
- ☐ Access Codes
- ☒ Override
- ☐ Tenanting

Explanation:

Override feature of PBS provides for the possibility to break into a busy line to inform another user an important message.

Licensed to Berend Post berend.post@it-university.nl

For CISA exam you should know below mentioned PBS features and Risks

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking

Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)

Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes

Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features

Silent Monitoring

Silently monitors other calls

Eavesdropping

Licensed to Berend Post berend.post@it-university.nl

Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference

override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping

Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting

Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail

Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release

Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Licensed to Berend Post berend.post@it-university.nl

Eavesdropping

No busy extension

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics

Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting

When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Account Codes - that are used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)

Licensed to Berend Post berend.post@it-university.nl

Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Access Codes - Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Tenanting - Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 358

Question 1369

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

- ☐ Embedded audit module
- ☐ Integrated test facility
- ☐ Snapshots
- ☒ Audit hooks

Explanation:

Explanation:

The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially-written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audit trail is required.

Licensed to Berend Post berend.post@it-university.nl

Question 1370

In-house personnel performing IS audits should possess which of the following knowledge and/or skills (Choose two.):

- ☒ information systems knowledge commensurate with the scope of the IT environment in question
- ☒ sufficient analytical skills to determine root cause of deficiencies in question
- ☐ sufficient knowledge on secure system coding
- ☐ sufficient knowledge on secure platform development
- ☐ information systems knowledge commensurate outside of the scope of the IT environment in question

Explanation:

Explanation:

Personnel performing IT audits should have information systems knowledge commensurate with the scope of the institution's IT environment. They should also possess sufficient analytical skills to determine the root cause of deficiencies.

Question 1371

Which of the following should be established FIRST when initiating a control self-assessment program in a small organization?

- ☐ Control baselines
- ☒ Client questionnaires
- ☐ External consultants
- ☐ Facilitated workshops

Question 1372

During a review of an organization's network threat response process, the IS auditor noticed that the majority of alerts were closed without resolution. Management responded that those alerts were unworkable due to lack of actionable intelligence, and therefore the support team is allowed to close them. What is the BEST way for the auditor to address this situation?

- ☒ Further review closed unactioned alerts to identify mishandling of threats.
- ☐ Omit the finding from the report as this practice is in compliance with the current policy.
- ☐ Recommend that management enhance the policy and improve threat awareness training.
- ☐ Reopen unactioned alerts and report to the audit committee.

Licensed to Berend Post berend.post@it-university.nl

Question 1373

From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

- ☐ a big bang deployment after proof of concept.
- ☐ prototyping and a one-phase deployment.
- ☒ a deployment plan based on sequenced phases.
- ☐ to simulate the new infrastructure before deployment.

Explanation:

Explanation:

When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

Question 1374

Which of the following ensures the availability of transactions in the event of a disaster?

- ☐ Send tapes hourly containing transactions offsite,
- ☐ Send tapes daily containing transactions offsite.
- ☐ Capture transactions to multiple storage devices.
- ☒ Transmit transactions offsite in real time.

Explanation:

Explanation:

The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

Question 1375

Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?

- ☐ Compensating controls in place to protect information security
- ☐ Corresponding breaches associated with each vendor
- ☒ Criticality of the service to the organization
- ☐ Compliance requirements associated with the regulation

Licensed to Berend Post berend.post@it-university.nl

Question 1376

When conducting a post-incident review, the GREATEST benefit of collecting mean time to resolution (MTTR) data is the ability to:

- ☐ reduce the costs of future preventive controls
- ☐ provide metrics for reporting to senior management
- ☐ verify compliance with the service level agreement (SLA)
- ☒ learn of potential areas of improvement

Question 1377

In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

- ☐ Message Switching
- ☐ Packet switching
- ☒ Circuit switching
- ☐ Virtual Circuits

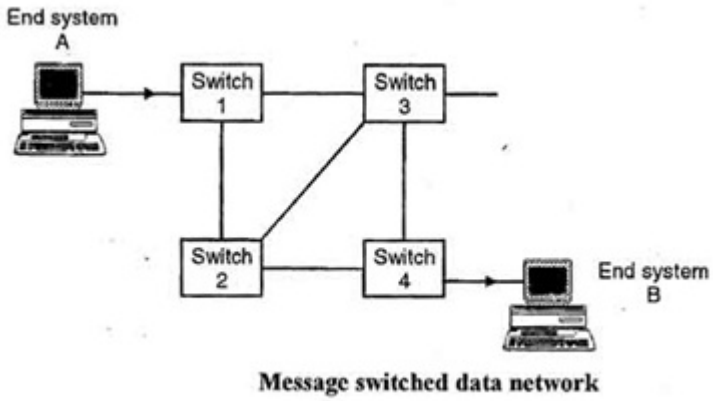
Explanation:

For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching



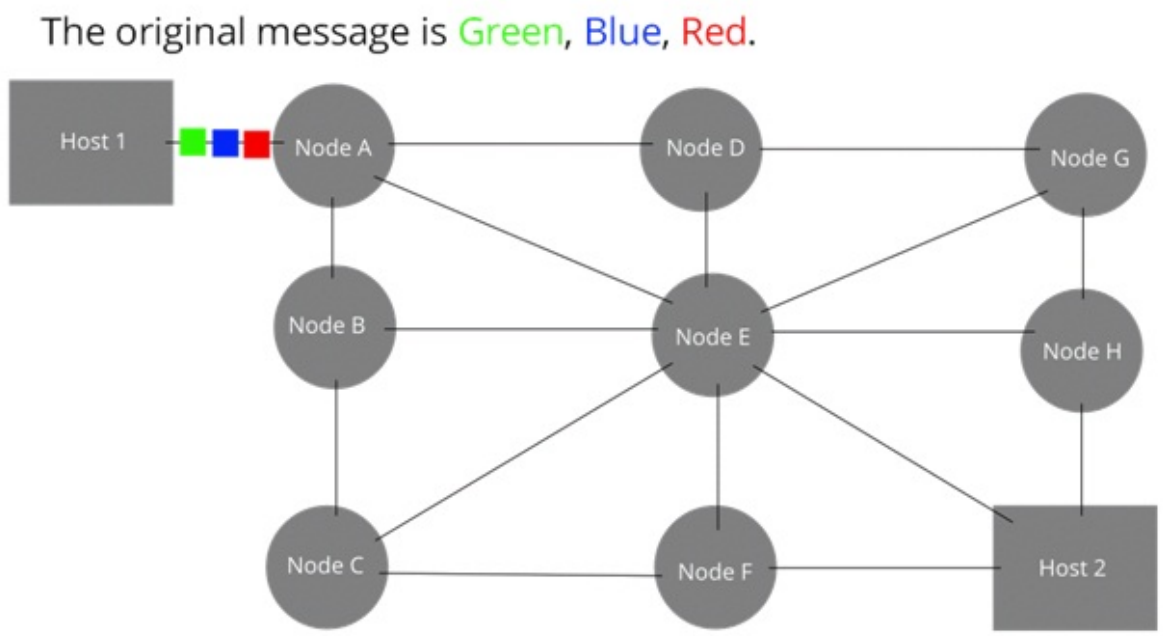
Message switched data network

Packet Switching

Licensed to Berend Post berend.post@it-university.nl

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching



Circuit Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

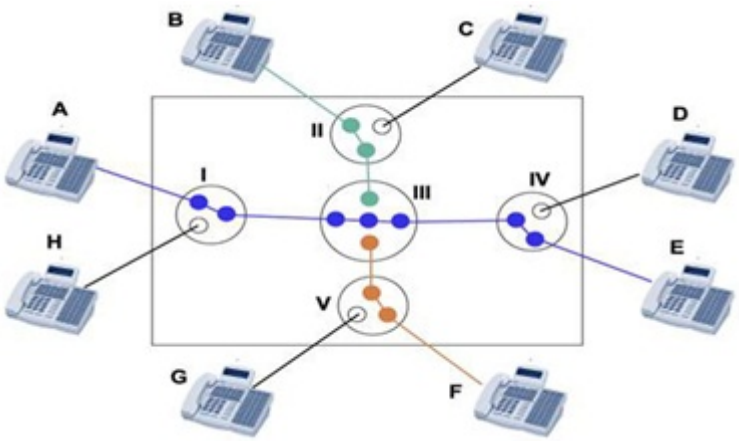
The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Licensed to Berend Post berend.post@it-university.nl

Circuit Switching



See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required

Licensed to Berend Post berend.post@it-university.nl

during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented are not valid choices.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

Question 1378

A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

- ☒ dials back to the user machine based on the user id and password using a telephone number from its database.
- ☐ dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.
- ☐ waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.
- ☐ waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's database.

Explanation:

Explanation:

A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and then the server disconnects and dials back to the user machine based on the user id and password using a telephone number from its database. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

Licensed to Berend Post berend.post@it-university.nl

Question 1379

Which of the following is a technique that could be used to capture network user passwords?

- ☐ Encryption
- ☒ Sniffing
- ☐ Spoofing
- ☐ Data destruction

Explanation:

Explanation: Sniffing is an attack that can be used to capture sensitive pieces of information (e.g., a password) passing through the network. Encryption is a method of scrambling information to prevent unauthorized individuals from understanding the transmission. Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication. Data destruction is erasing information or removing it from its original location.

Question 1380

A benefit of open system architecture is that it:

- ☒ facilitates interoperability.
- ☐ facilitates the integration of proprietary components.
- ☐ will be a basis for volume discounts from equipment vendors.
- ☐ allows for the achievement of more economies of scale for equipment.

Explanation:

Explanation:

Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

Question 1381

An organization has begun using social media to communicate with current and potential clients. Which of the following should be of PRIMARY concern to the auditor?

- ☐ Using a third-party provider to host and manage content
- ☒ Lack of guidance on appropriate social media usage and monitoring
- ☐ Negative posts by customers affecting the organization's image
- ☐ Reduced productivity of stuff using social media

Licensed to Berend Post berend.post@it-university.nl

Question 1382

Which of the following should be an information security manager's MOST important consideration when conducting a physical security review of a potential outsourced data center?

- ☒ Environmental factors of the surrounding location
- ☐ Proximity to law enforcement
- ☐ Availability of network circuit connections
- ☐ Distance of the data center from the corporate office

Question 1383

Which of the following layer of an OSI model controls dialog between computers?

- ☐ Application layer
- ☐ Presentation layer
- ☒ Session layer
- ☐ Transport layer

Explanation:

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

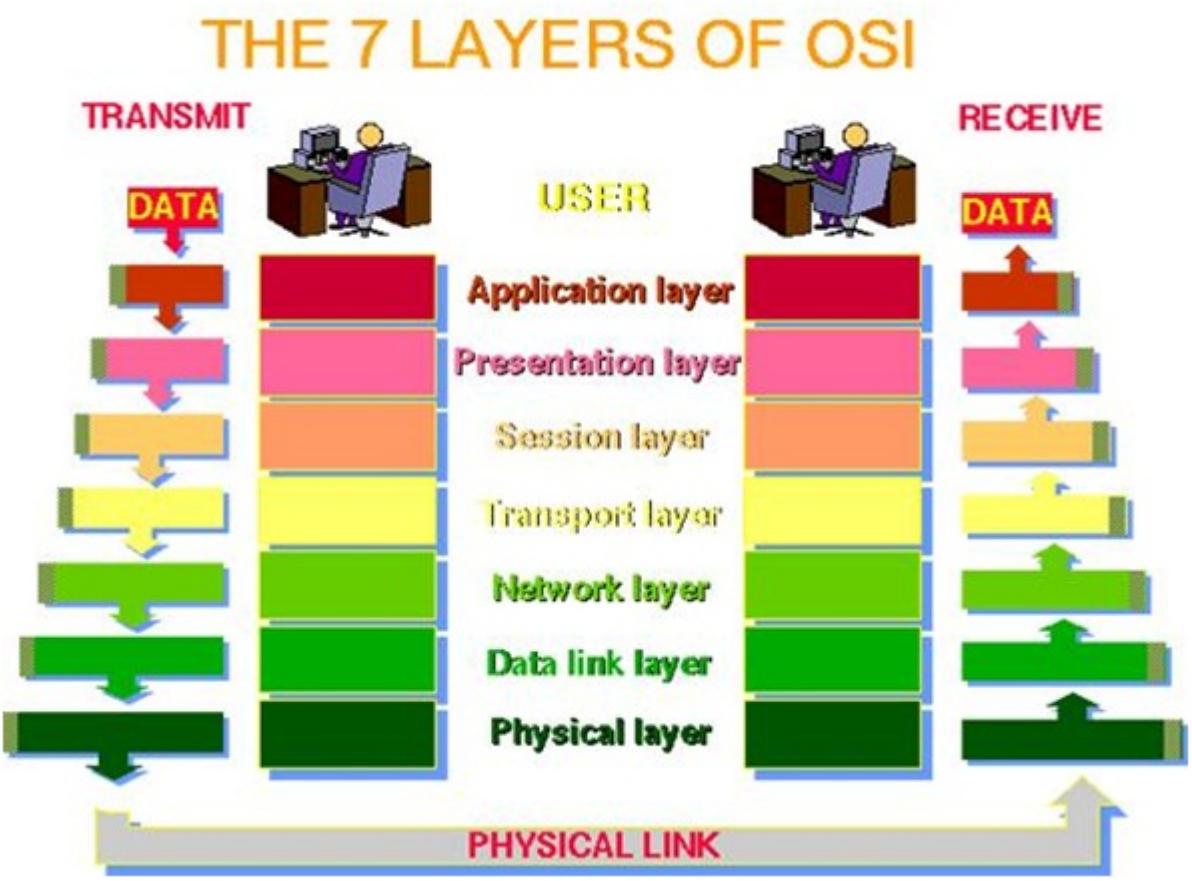
For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model

Licensed to Berend Post berend.post@it-university.nl



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Licensed to Berend Post berend.post@it-university.nl

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

Licensed to Berend Post berend.post@it-university.nl

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

Licensed to Berend Post berend.post@it-university.nl

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Application Layer - The application layer serves as the window for users and application processes to access network services.

Licensed to Berend Post berend.post@it-university.nl

Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Question 1384

Which of the following is the MOST important privacy consideration for an organization that uses a cloud service provider to process customer data?

- ☐ Data privacy must be monitored in accordance with industry standards and best practices.
- ☐ All customer data transferred to the service provider must be reported to the regulatory authority.
- ☐ No personal information may be transferred to the service provider without the consent of the customer.
- ☒ Data privacy must be managed in accordance with the regulations applicable to the organization.

Question 1385

Utilizing external resources for highly technical information security tasks allows an information security manager to:

- ☒ transfer business risk.
- ☐ distribute technology risk.
- ☐ outsource responsibility.
- ☐ leverage limited resources.

Licensed to Berend Post berend.post@it-university.nl

Question 1386

An organization's business continuity plan (BCP) should be:

- ☒ updated based on changes to personnel and environments.
- ☐ tested whenever new applications are implemented.
- ☐ tested after successful intrusions into the organization's hot site.
- ☐ updated only after independent audit review by a third party.

Question 1387

Which of the following control checks would utilize data analytics?

- ☐ Evaluating configuration settings for the credit card application system
- ☐ Reviewing credit card applications submitted in the past month for blank data fields
- ☐ Attempting to submit credit card applications with blank data fields
- ☒ Reviewing the business requirements document for the credit card application system

Question 1388

An IS auditor has completed an audit on the organization's IT strategic planning process. Which of the following findings should be given the HIGHEST priority?

- ☒ The IT strategic plan was completed prior to the formulation of the business strategic plan
- ☐ Assumptions in the IT strategic plan have not been communicated to business stakeholders
- ☐ The IT strategic plan was formulated based on the current IT capabilities
- ☐ The IT strategic plan does not include resource requirements for implementation

Question 1389

Which of the following is the MOST reliable sender authentication method?

- ☐ Digital signatures
- ☐ Asymmetric cryptography
- ☒ Digital certificates
- ☐ Message authentication code

Explanation:

Explanation:

Digital certificates are issued by a trusted third party. The message sender attaches the certificate and the recipient can verify authenticity with the certificate repository. Asymmetric cryptography, such as public key infrastructure (PKI), appears to authenticate the sender but is vulnerable to a man-in-the-middle attack. Digital signatures are used for both authentication and confidentiality, but the identity of the sender would still be confirmed by the digital certificate. Message authentication code is used for message integrity verification.

Licensed to Berend Post berend.post@it-university.nl

Question 1390

Business Continuity Planning (BCP) is not defined as a preparation that facilitates:

- ☐ the rapid recovery of mission-critical business operations
- ☐ the continuation of critical business functions
- ☒ the monitoring of threat activity for adjustment of technical controls
- ☐ the reduction of the impact of a disaster

Explanation:

The following answers are incorrect:

All of the other choices are facilitated by a BCP:

the continuation of critical business functions

the rapid recovery of mission-critical business operations

the reduction of the impact of a disaster

Question 1391

Which of the following typically consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared?

- ☒ honeypot
- ☐ superpot
- ☐ IDS
- ☐ IPS
- ☐ firewall
- ☐ None of the choices.

Explanation:

Explanation:

You may use a honeypot to detect and deflect unauthorized use of your information systems. A typical honeypot consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared for trapping hackers.

Licensed to Berend Post berend.post@it-university.nl

Question 1392

Which of the following control provides an alternative measure of control?

- ☐ Deterrent
- ☐ Preventive
- ☐ Detective
- ☒ Compensating

Explanation:

Explanation:

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

Licensed to Berend Post berend.post@it-university.nl

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to

find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other

technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective

nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

Licensed to Berend Post berend.post@it-university.nl

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security

incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take

many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

Licensed to Berend Post berend.post@it-university.nl

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Licensed to Berend Post berend.post@it-university.nl

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Licensed to Berend Post berend.post@it-university.nl

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring

Detective -Detective control helps identify an incident's activities and potentially an intruder

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 1393

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

- ☐ Personally delete all copies of the unauthorized software.
- ☐ Inform the auditee of the unauthorized software, and follow up to confirm deletion.
- ☒ Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
- ☐ Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Explanation:

Explanation:

The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

Licensed to Berend Post berend.post@it-university.nl

Question 1394

Which of the following analytical methods would be MOST useful when trying to identify groups with similar behavior or characteristics in a large population?

- ☐ Classification
- ☒ Correlation analysis
- ☐ Deviation detection
- ☐ Clustering

Question 1395

Several remote users have been unable to communicate with a secured network news transfer protocol (NNTP) server. Of the following, the MOST likely cause is:

- ☐ the use of a password cracker
- ☒ a hacker impersonating the server
- ☐ a hacker using a sniffer
- ☐ a replay attack by an eavesdropper

Question 1396

Which of the following type of network service is used by network computer to obtain an IP addresses and other parameters such as default gateway, subnet mask?

- ☒ DHCP
- ☐ DNS
- ☐ Directory Service
- ☐ Network Management

Explanation:

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client

Licensed to Berend Post berend.post@it-university.nl

components running on other devices. However, the client and server components can both be run on the same machine.

Clients and servers will often have a user interface, and sometimes other hardware associated with them.

Different types of network services are as follows:

Network File System - Network File System (NFS) is a distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a network much like local storage is accessed.

Remote Access Service - Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

Directory Services - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.

Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:

Directory Service - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

 Licensed to Berend Post berend.post@it-university.nl

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Question 1397

Which of the following BEST ensures that only authorized software is moved into a production environment?

- ☐ Restricting read/write access to production code to computer programmers only
- ☒ Assigning programming managers to transfer tested programs to production
- ☐ A librarian compiling source code into production after independent testing
- ☐ Requiring programming staff to move tested code into production

Question 1398

ALL computer programming languages are vulnerable to command injection attack.

- ☐ True
- ☒ False

Explanation:

Explanation:

The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

Question 1399

Test and development environments should be separated. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Test and development environments should be separated, to control the stability of the test environment.

Question 1400

An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

- ☒ professional independence
- ☐ organizational independence.
- ☐ technical competence.
- ☐ professional competence.

Explanation:

Explanation:

When an IS auditor recommends a specific vendor, they compromise professional independence. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement. Technical and professional competence is not relevant to the requirement of independence.

Question 1401

Which of the following presents the GREATEST concern when implementing data flow across borders?

- ☐ Software piracy laws
- ☒ National privacy laws
- ☐ Political unrest
- ☐ Equipment incompatibilities

Question 1402

Which of the following is the BEST indicator of an effective employee information security program?

- ☐ Increased management support for security
- ☒ More efficient and effective incident handling
- ☐ Increased detection and reporting of incidents
- ☐ Reduced operational cost of security

Licensed to Berend Post berend.post@it-university.nl

Question 1403

Which of the following is MOST effective in the strategic alignment of security initiatives?

- ☐ A security steering committee is set up within the IT department.
- ☐ Key information security policies are updated on a regular basis.
- ☐ Business leaders participate in information security decision making.
- ☒ Policies are created with input from business unit managers.

Question 1404

An internal review reveals an out-of-support human resources system. Which of the following is MOST important to determine when evaluating the associated risk?

- ☐ Frequency of outages associated with the out-of-support system
- ☐ The number of people accessing the out-of-support system
- ☐ Exposure of the out-of-support system outside of the network
- ☒ Timeline to replace the out-of-support system

Question 1405

The PRIMARY purpose of a business impact analysis (BIA) is to:

- ☐ provide a plan for resuming operations after a disaster.
- ☒ identify the events that could impact the continuity of an organization's operations.
- ☐ publicize the commitment of the organization to physical and logical security.
- ☐ provide the framework for an effective disaster recovery plan.

Explanation:

Explanation:

A business impact analysis (BIA) is one of the key steps in the development of a business continuity plan (BCP). A BIA will identify the diverse events that could impact the continuity of the operations of an organization.

Question 1406

Which of the following is the GREATEST advantage of application penetration testing over vulnerability scanning?

- ☐ Penetration testing does not require a special skill set to be executed.
- ☒ Penetration testing provides a more accurate picture of gaps in application controls.
- ☐ Penetration testing can be conducted in a relatively short time period.
- ☐ Penetration testing creates relatively smaller risks to application availability and integrity.

Licensed to Berend Post berend.post@it-university.nl

Question 1407

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- ☐ Function point analysis
- ☒ PERT chart
- ☐ Rapid application development
- ☐ Object-oriented system development

Explanation:

Explanation:

A PERT chart will help determine project duration once all the activities and the work involved with those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

Question 1408

Which of the following is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization?

- ☒ Private Branch Exchange
- ☐ Virtual Local Area Network
- ☐ Voice over IP
- ☐ Dial-up connection

Explanation:

A Private Branch Exchange(PBX) is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization that operates it. Protection of PBX is thus a height priority. Failure to secure PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, loss of revenue or legal entanglements.

PBX environment involves many security risks, presented by people both internal and external to an organization. The threat of the PBX telephone system is many, depending on the goals of these attackers, and include:

Theft of service - Toll fraud, probably the most common of motives for attacker.

Licensed to Berend Post berend.post@it-university.nl

Disclosure of Information -Data disclosed without authorization, either by deliberate actionably accident. Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Data Modification -Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access – Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service -Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Traffic Analysis – A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

Virtual Local Area Network - A virtual local area network (VLAN) is a logical group of workstations, servers and network devices that appear to be on the same LAN despite their geographical distribution. A VLAN allows a network of computers and users to communicate in a simulated environment as if they exist in a single LAN and are sharing a single broadcast and multicast domain. VLANs are implemented to achieve scalability, security and ease of network management and can quickly adapt to change in network requirements and relocation of workstations and server nodes.

Voice over IP - VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitalized into IP packets and transferred through the network layer before being decode back into the original voice.

Dial-up connection - Dial-up refers to an Internet connection that is established using a modem. The modem connects the computer to standard phone lines, which serve as the data transfer medium. When a user initiates a dial-up connection, the modem dials a phone number of an Internet Service Provider (ISP) that is designated to receive dial-up calls. The ISP then establishes the connection, which usually takes about ten seconds and is accompanied by several beeping an buzzing sounds.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 356

Question 1409

The PRIMARY objective of testing a business continuity plan is to:

- ☐ familiarize employees with the business continuity plan.
- ☐ ensure that all residual risks are addressed.
- ☐ exercise all possible disaster scenarios.
- ☒ identify limitations of the business continuity plan.

Explanation:

Explanation:

Testing the business continuity plan provides the best evidence of any limitations that may exist. Familiarizing employees with the business continuity plan is a secondary benefit of a test. It is not cost effective to address residual risks in a business continuity plan, and it is not practical to test all possible disaster scenarios.

Question 1410

Which of the following is MOST important for an information security manager to ensure is included in a business case for a new system?

- ☒ Intangible benefits of the system
- ☐ Risk associated with the system
- ☐ Effectiveness of controls
- ☐ Audit-logging capabilities

Question 1411

The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- ☐ Utilization of an intrusion detection system to report incidents
- ☐ Mandating the use of passwords to access all software
- ☐ Installing an efficient user log system to track the actions of each user
- ☒ Training provided on a regular basis to all current and new employees

Explanation:

Explanation:

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

Licensed to Berend Post berend.post@it-university.nl

Question 1412

When conducting a follow-up of previous audit findings, an IS auditor is told by management that a recommendation to make security changes to an application has not been implemented. The IS auditor should FIRST determine whether:

- ☒ additional time to implement changes is needed.
- ☐ the associated risk is still relevant.
- ☐ the recommendation should be re-issued.
- ☐ the issue should be escalated.

Question 1413

Who is responsible for the overall direction, costs, and timetables for systems-development projects?

- ☐ The project sponsor
- ☒ The project steering committee
- ☐ Senior management
- ☐ The project team leader

Explanation:

Explanation:

The project steering committee is responsible for the overall direction, costs, and timetables for systems-development projects.

Question 1414

The PRIMARY role of a control self-assessment (CSA) facilitator is to:

- ☒ report on the internal control weaknesses.
- ☐ focus the team on internal controls.
- ☐ provide solutions for control weaknesses.
- ☐ conduct interviews to gain background information.

Licensed to Berend Post berend.post@it-university.nl

Question 1415

_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

- ☒ Quantitative; qualitative
- ☐ Qualitative; quantitative
- ☐ Residual; subjective
- ☐ Quantitative; subjective

Explanation:

Explanation:

Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

Question 1416

Which of the following ACID property in DBMS means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☒ Durability

Explanation:

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Licensed to Berend Post berend.post@it-university.nl

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction. [citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

The following were incorrect answers:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 218

Licensed to Berend Post berend.post@it-university.nl

Question 1417

Nonrepudiation of the client for e-commerce transactions is accomplished through which of the following control mechanisms?

- ☐ Password security
- ☐ Internet protocol (IP) address verification
- ☒ Public key infrastructure (PKI)
- ☐ Secure Sockets Layer (SSL)

Question 1418

An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

- ☐ more than one individual can claim to be a specific user.
- ☒ there is no way to limit the functions assigned to users.
- ☐ user accounts can be shared.
- ☐ users have a need-to-know privilege.

Explanation:

Explanation:

Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

Question 1419

The decision to accept an IT control risk related to data quality should be the responsibility of the:

- ☒ information security team
- ☐ chief information officer
- ☐ business owner
- ☐ IS audit manager

Question 1420

The MOST useful technique for maintaining management support for the information security program is:

- ☒ identifying the risks and consequences of failure to comply with standards
- ☐ benchmarking the security programs of comparable organizations
- ☐ implementing a comprehensive security awareness and training program
- ☐ informing management about the security of business operations

Licensed to Berend Post berend.post@it-university.nl

Question 1421

What is the MOST effective way to ensure security policies and procedures are up-to-date?

- ☐ Verify security requirements are being identified and consistently applied.
- ☒ Align the organization's security practices with industry standards and best practice.
- ☐ Define and document senior management's vision for the direction of the security
- ☐ Prevent security documentation audit issues from being raised

Question 1422

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☒ MTD

Explanation:

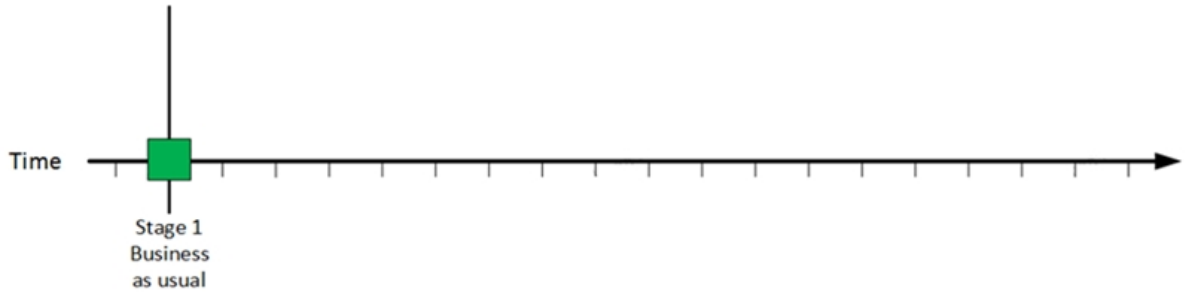
Explanation:

The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

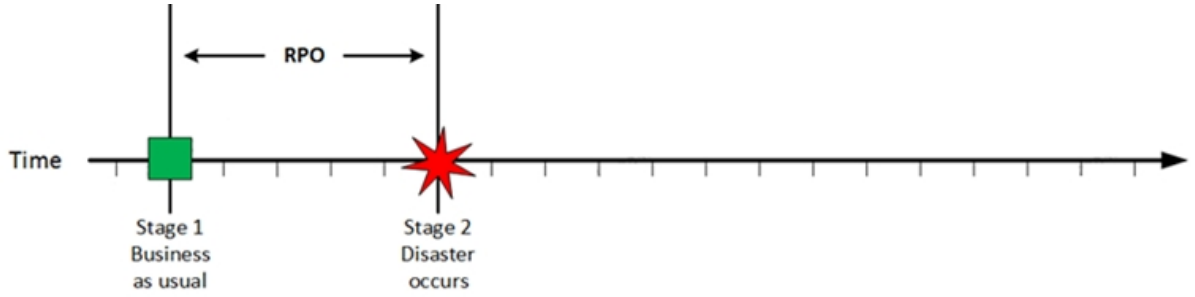


At this stage all systems are running production and working correctly.

Licensed to Berend Post berend.post@it-university.nl

Stage 2: Disaster occurs

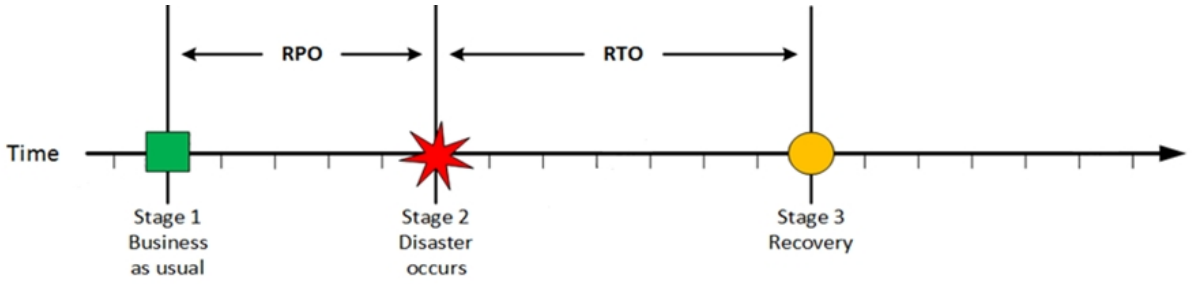
Disaster Occurs



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

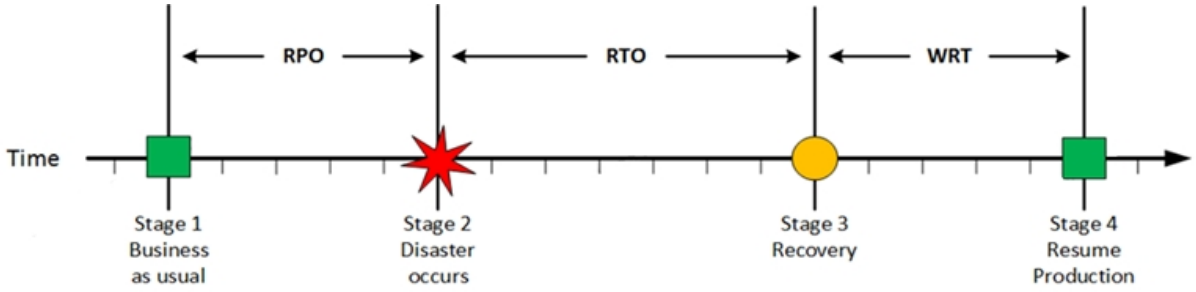


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

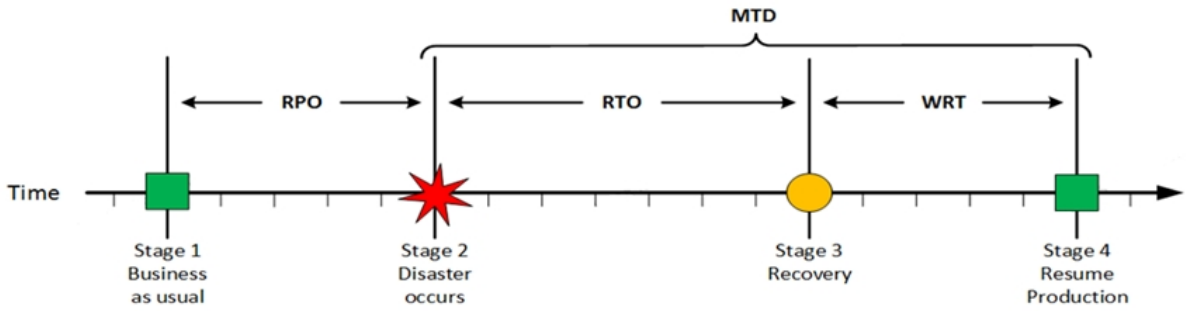
Resume Production

Licensed to Berend Post berend.post@it-university.nl



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up

Licensed to Berend Post berend.post@it-university.nl

or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

References:

CISA review manual 2014 page number 284

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 1423

The reliability of an application system's audit trail may be questionable if:

- ☐ user IDs are recorded in the audit trail.
- ☐ the security administrator has read-only rights to the audit file.
- ☐ date and time stamps are recorded when an action occurs.
- ☒ users can amend audit trail records when correcting system errors.

Explanation:

Explanation:

An audit trail is not effective if the details in it can be amended.

Question 1424

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing.
True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing.

Question 1425

Which of the following should be done FIRST to effectively define the IT audit universe for an entity with multiple business lines?

- ☐ Identify aggregate residual IT risk for each business line.
- ☐ Obtain a complete listing of the entity's IT processes.
- ☐ Obtain a complete listing of assets fundamental to the entity's businesses.
- ☒ Identify key control objectives for each business line's core processes.

Question 1426

Which of the following is MOST likely to prevent social engineering attacks?

- ☒ Security awareness program
- ☐ Employee background checks
- ☐ Implementing positive identification policies
- ☐ Enforcing stronger hiring policies

Question 1427

An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

- ☐ defining the conceptual schema.
- ☐ defining security and integrity checks.
- ☐ liaising with users in developing data model.
- ☒ mapping data model with the internal schema.

Explanation:

Explanation:

A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprise wide view of data within an organization and is the basis for deriving and end-user department data model.

Licensed to Berend Post berend.post@it-university.nl

Question 1428

Which of the following is MOST important for an IS auditor to review when evaluating the effectiveness of an organization's incident response process?

- ☐ Past incident response actions
- ☐ Incident response staff experience and qualifications
- ☒ Results from management testing of incident response procedures
- ☐ Incident response roles and responsibilities

Question 1429

How often should a Business Continuity Plan be reviewed?

- ☐ At least once a month
- ☐ At least every six months
- ☒ At least once a year
- ☐ At least Quarterly

Explanation:

As stated in SP 800-34 Rev. 1:

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.

Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within your exam.

Reference(s) used for this question:

NIST SP 800-34 Revision 1

Licensed to Berend Post berend.post@it-university.nl

Question 1430

Which of the following would MOST effectively enhance the security of a challenge- response based authentication system?

- ☐ Selecting a more robust algorithm to generate challenge strings
- ☒ implementing measures to prevent session hijacking attacks
- ☐ increasing the frequency of associated password changes
- ☐ increasing the length of authentication strings

Explanation:

Explanation:

Challenge response-based authentication is prone to session hijacking or man-in-the- middle attacks. Security management should be aware of this and engage in risk assessment and control design when they employ this technology. Selecting a more robust algorithm will enhance the security; however, this may not be as important in terms of risk when compared to man-in- the-middle attacks. Choices C and D are good security practices; however, they are not as effective a preventive measure. Frequently changing passwords is a good security practice; however, the exposures lurking in communication pathways may pose a greater risk.

Question 1431

What is the best defense against Distributed DoS Attack?

- ☒ patch your systems.
- ☐ run a virus checker.
- ☐ run an anti-spy software.
- ☐ find the DoS program and kill it.
- ☐ None of the choices.

Explanation:

Explanation:

Distributed DoS Attack is a network-based attack from many servers used remotely to send packets. Examples of tools for conducting such attack include TFN, TFN2K, Trin00, Stacheldracht, and variants. The best defense is to make sure all systems patches are up-to-date. Also make sure your firewalls are configured appropriately.

Question 1432

Which of the following type of a computer network covers a broad area such as city, region, nation or international link?

- ☐ LAN
- ☒ WAN
- ☐ SAN
- ☐ PAN

Explanation:

Licensed to Berend Post berend.post@it-university.nl

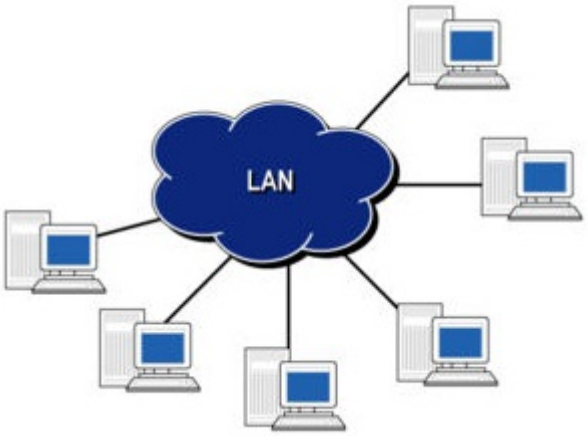
A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

Local Area Network

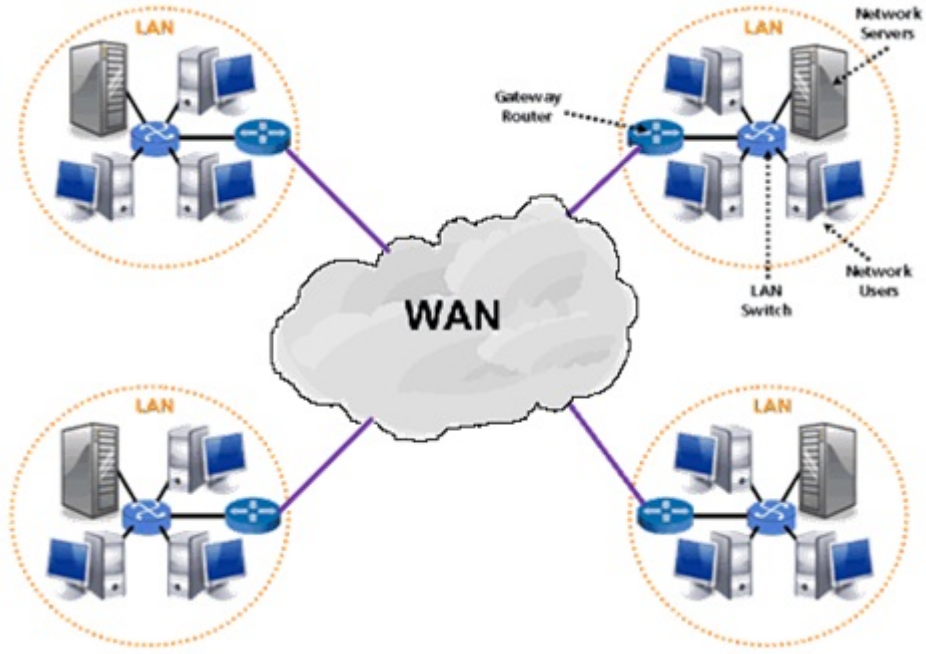


Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Wide Area Network

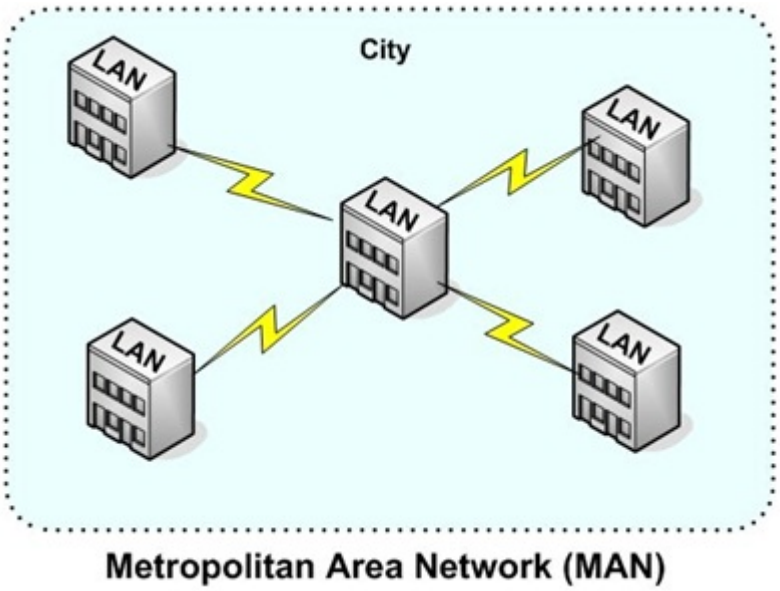
Licensed to Berend Post berend.post@it-university.nl



Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

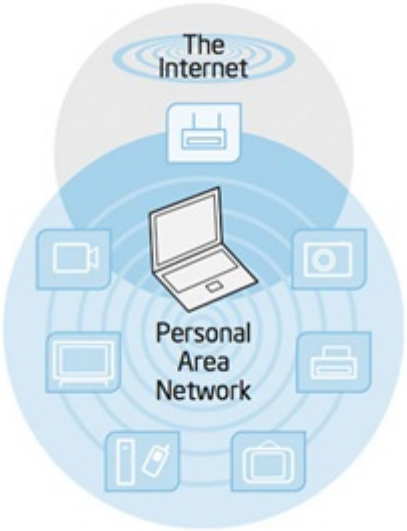


Personal Area Network

Licensed to Berend Post berend.post@it-university.nl

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

Licensed to Berend Post berend.post@it-university.nl

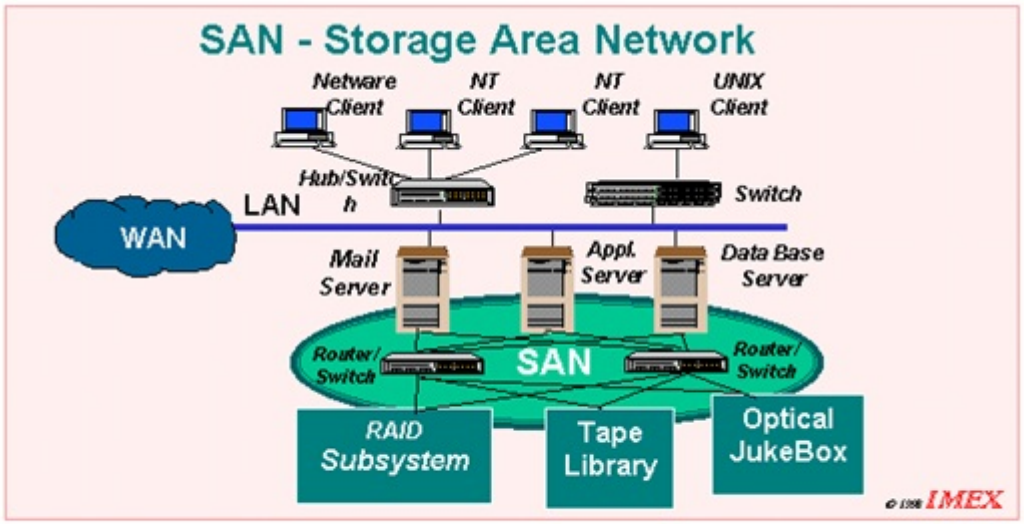


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Licensed to Berend Post berend.post@it-university.nl

Question 1433

Which of the following provides nonrepudiation services for e-commerce transactions?

- ☒ Public key infrastructure (PKI)
- ☐ Data Encryption Standard (DES)
- ☐ Message authentication code (MAC)
- ☐ Personal identification number (PIN)

Explanation:

Explanation: PKI is the administrative infrastructure for digital certificates and encryption key pairs. The qualities of an acceptable digital signature are: it is unique to the person using it; it is capable of verification; it is under the sole control of the person using it; and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The Data Encryption Standard (DES) is the most common private key cryptographic system. DES does not address nonrepudiation. A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission; it has nothing to do with nonrepudiation. A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

Question 1434

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- ☐ identify and assess the risk assessment process used by management.
- ☐ identify information assets and the underlying systems.
- ☐ disclose the threats and impacts to management.
- ☒ identify and evaluate the existing controls.

Explanation:

Explanation:

It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

Licensed to Berend Post berend.post@it-university.nl

Question 1435

While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

- ☐ A scan of all floppy disks before use
- ☐ A virus monitor on the network file server
- ☒ Scheduled daily scans of all network drives
- ☐ A virus monitor on the user's personal computer

Explanation:

Explanation:

Scheduled daily scans of all network drives will detect the presence of a virus after the infection has occurred. All of the other choices are controls designed to prevent a computer virus from infecting the system.

Question 1436

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- ☐ incorporates state of the art technology.
- ☐ addresses the required operational controls.
- ☒ articulates the IT mission and vision.
- ☐ specifies project management practices.

Explanation:

Explanation:

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

Question 1437

The scheduling of audit follow-ups should be based PRIMARILY on:

- ☐ costs and audit efforts involved.
- ☐ auditee and auditor time commitments.
- ☒ the risk and exposure involved.
- ☐ control and detection processes.

Licensed to Berend Post berend.post@it-university.nl

Question 1438

Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

- ☐ Client logins are subject to replay attack.
- ☐ VPN traffic could be sniffed and captured.
- ☒ Compromised VPN clients could impact the network.
- ☐ Attackers could compromise the VPN gateway.

Question 1439

The PRIMARY purpose of a periodic threat and risk assessment report to senior management is to communicate the:

- ☐ cost-benefit of security controls.
- ☒ status of the security posture.
- ☐ probability of future incidents.
- ☐ risk acceptance criteria.

Question 1440

Who should be responsible for network security operations?

- ☐ Business unit managers
- ☒ Security administrators
- ☐ Network administrators
- ☐ IS auditors

Explanation:

Explanation:

Security administrators are usually responsible for network security operations.

Question 1441

Which of the following is MOST important for the successful establishment of a security vulnerability management program?

- ☒ A comprehensive asset inventory
- ☐ A tested incident response plan
- ☐ An approved patching policy
- ☐ A robust tabletop exercise plan

Licensed to Berend Post berend.post@it-university.nl

Question 1442

An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager's FIRSTstep to support this strategy?

- ☐ Develop a business case for a data loss prevention solution
- ☒ Develop a guideline on the acceptable use of social media
- ☐ Incorporate social media into the security awareness program
- ☐ Employ the use of a web content filtering solution

Question 1443

An enterprise receiving email should have procedures to control:

- ☐ insufficient end-points.
- ☒ unsolicited executable code.
- ☐ outdated protocols.
- ☐ insufficient connectivity.

Question 1444

As part of an audit response, an auditee has concerns with the recommendations and is hesitant to implement them. Which of the following would be the BEST course of action for the IS auditor?

- ☐ Accept the auditee's response and perform additional testing.
- ☒ Conduct further discussions with the auditee to develop a mitigation plan.
- ☐ Suggest hiring a third-party consultant to perform a current state assessment.
- ☐ Issue a final report without including the opinion of the auditee.

Question 1445

After implementation of a disaster recovery plan, pre-disaster and post-disaster operational costs for an organization will:

- ☐ decrease.
- ☐ not change (remain the same).
- ☒ increase.
- ☐ increase or decrease depending upon the nature of the business.

Explanation:

Explanation:

There are costs associated with all activities and disaster recovery planning (DRP) is not an exception. Although there are costs associated with a disaster recovery plan, there are unknown costs that are incurred if a disaster recovery plan is not implemented.

Licensed to Berend Post berend.post@it-university.nl

Question 1446

The BEST way to avoid session hijacking is to use:

- ☐ a reverse lookup
- ☒ a secure protocol
- ☐ a firewall
- ☐ strong password controls

Question 1447

Who is responsible for reviewing the result and deliverables within and at the end of each phase, as well as confirming compliance with requirements?

- ☐ Project Sponsor
- ☒ Quality Assurance
- ☐ User Management
- ☐ Senior Management

Explanation:

Quality Assurance personnel review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

For CISA exam you should know below information about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management -Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?

How reliable is the software?

How effective is the software?

Is the software easy to use?

Licensed to Berend Post berend.post@it-university.nl

How easy is to transfer or adapt old data from preexisting software to this environment?

Is it possible to add new functions?

Does it meet regulatory requirement?

Project Steering Committee -Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

System Development Management -Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager -Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor - Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team -Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team -Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Licensed to Berend Post berend.post@it-university.nl

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Project Sponsor - Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

User Management - Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 150

Question 1448

Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

- ☐ A user from within could send a file to an unauthorized person.
- ☐ FTP services could allow a user to download files from unauthorized sources.
- ☒ A hacker may be able to use the FTP service to bypass the firewall.
- ☐ FTP could significantly reduce the performance of a DMZ server.

Explanation:

Explanation:

Since file transfer protocol (FTP) is considered an insecure protocol, it should not be installed on a server in a demilitarized zone (DMZ). FTP could allow an unauthorized user to gain access to the

Licensed to Berend Post berend.post@it-university.nl

network. Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

Question 1449

Default permit is only a good approach in an environment where:

- ☒ security threats are non-existent or negligible.
- ☐ security threats are non-negligible.
- ☐ security threats are serious and severe.
- ☐ users are trained.
- ☐ None of the choices.

Explanation:

Explanation:

"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality. This is a good approach if you have lots of security threats. On the other hand, ""Everything not explicitly forbidden is permitted"" (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non-existent or negligible."

Question 1450

Security should ALWAYS be an all or nothing issue.

- ☐ True
- ☐ True for trusted systems only
- ☐ True for untrusted systems only
- ☒ False
- ☐ None of the choices.

Explanation:

Explanation:

Security should not be an all or nothing issue. The designers and operators of systems should assume that security breaches are inevitable in the long term. Full audit trails should be kept of system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined.

Licensed to Berend Post berend.post@it-university.nl

Question 1451

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- ☐ establishment of a review board.
- ☐ creation of a security unit.
- ☒ effective support of an executive sponsor.
- ☐ selection of a security process owner.

Explanation:

Explanation:

The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is the most critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

Question 1452

Which of the following statement INCORRECTLY describes device and where they sit within the TCP/IP model?

- ☒ Layer 4 switch work at Network interface layer in TCP/IP model
- ☐ Router works at Network interface layer in TCP/IP model
- ☐ Layer 3 switch work at Network interface layer in TCP/IP model
- ☐ Hub works at LAN or WAN interface layer of a TCP/IP model

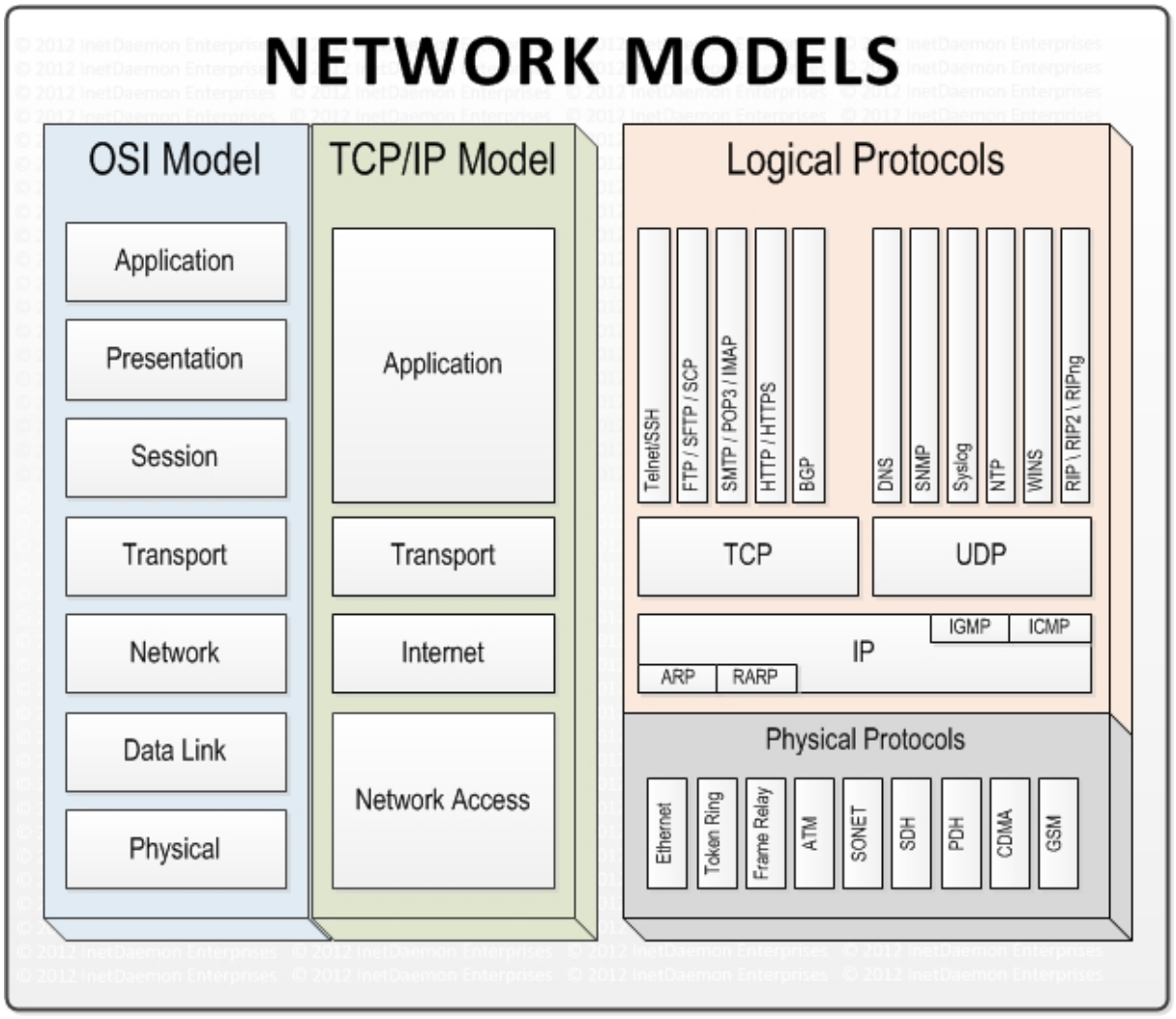
Explanation:

The keyword within the question is INCORRECTLY. You need to find out incorrect statement.

For your exam you should know below information about TCP/IP model:

Network models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

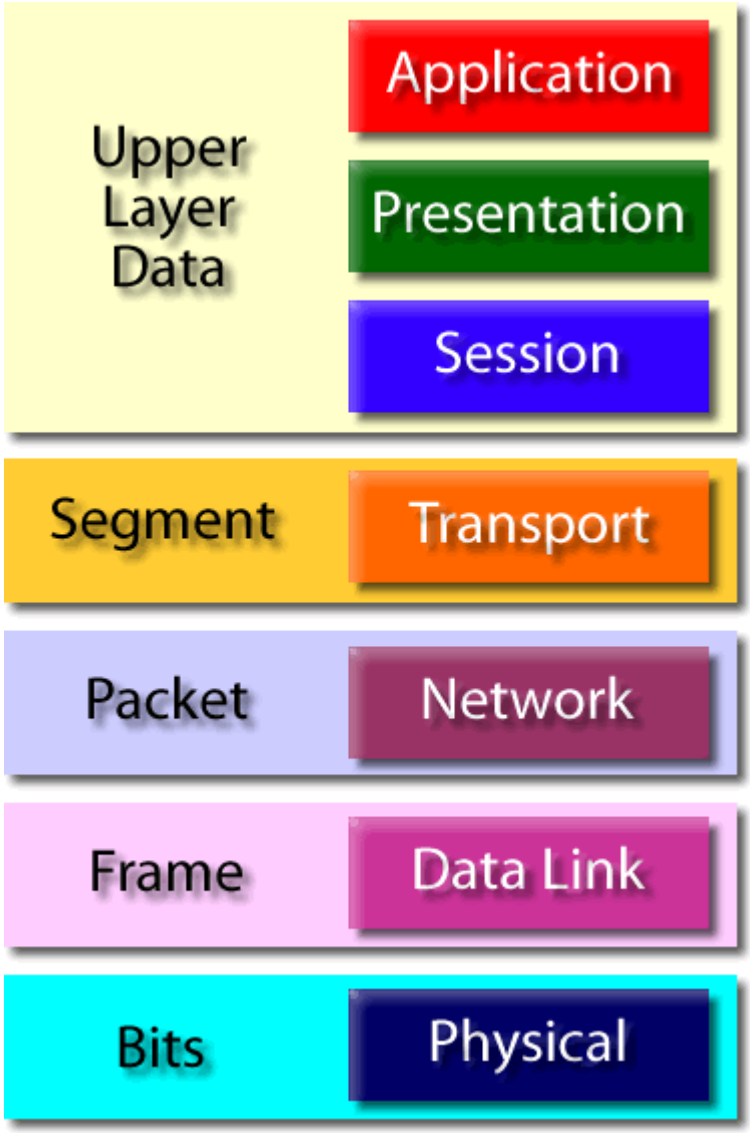
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :



Licensed to Berend Post berend.post@it-university.nl

Protocol Data Unit - PDU

The following answers are incorrect:

The other options correctly describe about network device functioning based on TCP/IP model

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 1453

Which of the following is the MOST reliable way for an IS auditor to evaluate the operational effectiveness of an organization's data loss prevention (DLP) controls?

- ☐ Verify that confidential files cannot be transmitted to a personal USB device.
- ☐ Conduct interviews to identify possible data protection vulnerabilities.
- ☒ Review data classification levels based on industry best practice.
- ☐ Verify that current DLP software is installed on all computer systems.

Question 1454

When designing metrics for information security, the MOST important consideration is that the metrics:

- ☐ provide actionable data.
- ☐ apply to all business units.
- ☐ are easy to understand.
- ☒ track trends over time.

Explanation:

Reference: https://m.isaca.org/Journal/archives/2016/volume-6/Documents/Journal-volume-6-2016.pdf

Question 1455

An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

- ☐ Analyze the need for the structural change.
- ☐ Recommend restoration to the originally designed structure.
- ☐ Recommend the implementation of a change control process.
- ☒ Determine if the modifications were properly approved.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

An IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the IS auditor find that the structural modification had not been approved.

Question 1456

Which of the following should be of GREATEST concern to an IS auditor reviewing actions taken during a forensic investigation?

- ☐ The investigation report does not indicate a conclusion.
- ☐ An image copy of the attacked system was not taken.
- ☒ The proper authorities were not notified.
- ☐ The handling procedures of the attacked system are not documented.

Question 1457

In which of the following WAN message transmission technique messages are divided into packets before they are sent and each packet is then transmitted individually and can even follow different routes to its destination?

- ☐ Message Switching
- ☒ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Explanation:

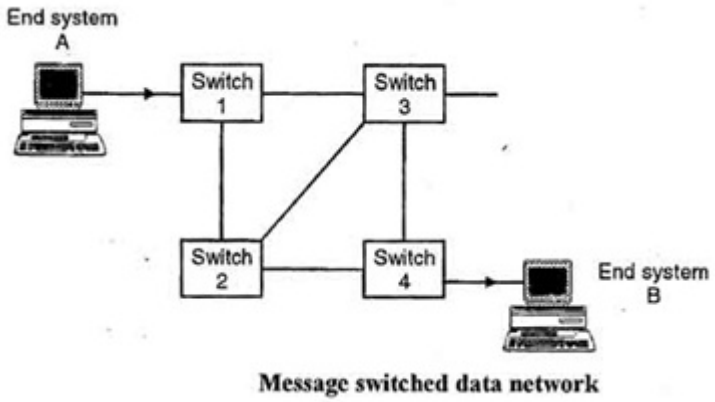
For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching

Licensed to Berend Post berend.post@it-university.nl

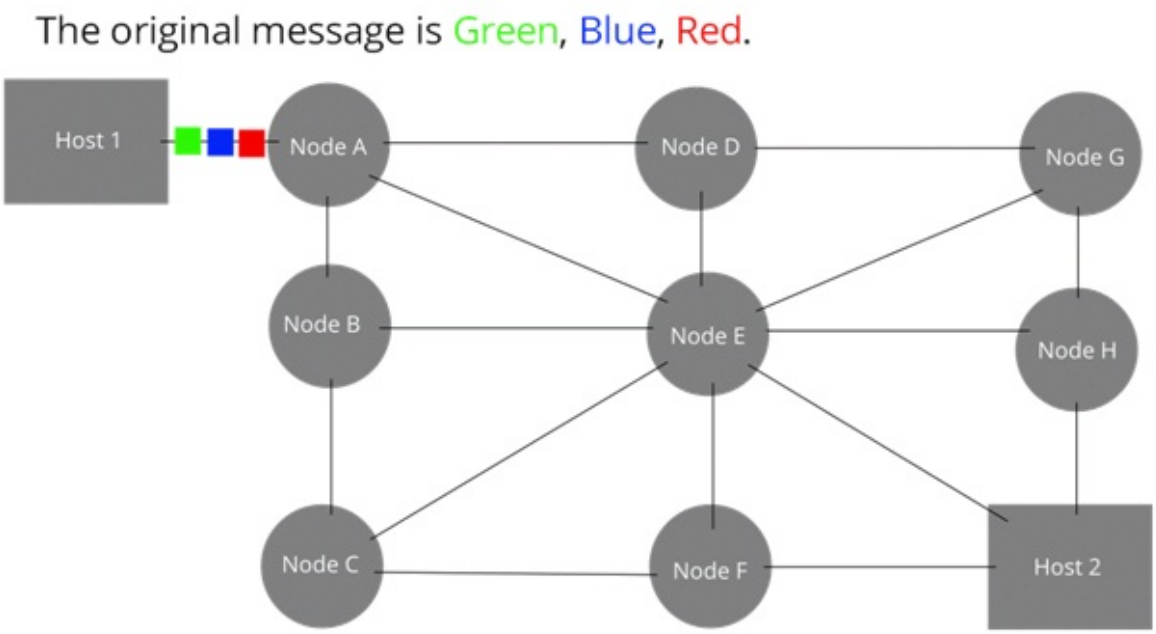


Message switched data network

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching



Circuit Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

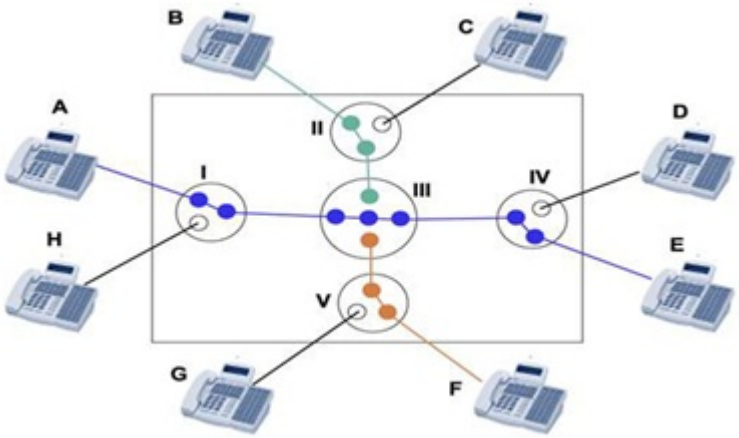
Licensed to Berend Post berend.post@it-university.nl

The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching



See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Licensed to Berend Post berend.post@it-university.nl

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented are not valid choices.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

Question 1458

Use of asymmetric encryption in an internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

- ☒ customer over the authenticity of the hosting organization.
- ☐ hosting organization over the authenticity of the customer.
- ☐ customer over the confidentiality of messages from the hosting organization.
- ☐ hosting organization over the confidentiality of messages passed to the customer.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Any false site will not be able to encrypt using the private key of the real site, so the customer would not be able to decrypt the message using the public key. Many customers have access to the same public key so the host cannot use this mechanism to ensure the authenticity of the customer. The customer cannot be assured of the confidentiality of messages from the host as many people have access to the public key and can decrypt the messages from the host. The host cannot be assured of the confidentiality of messages sent out, as many people have access to the public key and can decrypt it.

Question 1459

Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

- ☐ Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.
- ☒ Job descriptions contain clear statements of accountability for information security.
- ☐ In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
- ☐ No actual incidents have occurred that have caused a loss or a public embarrassment.

Explanation:

Explanation:

Inclusion in job descriptions of security responsibilities is a form of security training and helps ensure that staff and management are aware of their roles with respect to information security. The other three choices are not criterion for evaluating security awareness training. Awareness is a criterion for evaluating the importance that senior management attaches to information assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed, while the number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.

Question 1460

When facilitating the alignment of corporate governance and information security governance, which of the following is the MOST important role of an organization’s security steering committee?

- ☐ Obtaining support for the integration from business owners
- ☐ Obtaining approval for the information security budget
- ☒ Evaluating and reporting the degree of integration
- ☐ Defining metrics to demonstrate alignment

Licensed to Berend Post berend.post@it-university.nl

Question 1461

What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

- ☐ Business risk
- ☒ Detection risk
- ☐ Residual risk
- ☐ Inherent risk

Explanation:

Explanation:

Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

Question 1462

Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

- ☒ Increased; a greater
- ☐ Increased; a fewer
- ☐ Less; a fewer
- ☐ Increased; the same

Explanation:

Explanation:

Business process re-engineering often results in increased automation, which results in a greater number of people using technology.

Question 1463

An organization's HR department would like to outsource its employee management system to a cloud-hosted solution due to features and cost savings offered. Management has identified this solution as a business need and wants to move forward. What should be the PRIMARY role of information security in this effort?

- ☐ Ensure a security audit is performed of the service provider.
- ☐ Ensure the service provider has the appropriate certifications.
- ☒ Determine how to securely implement the solution.
- ☐ Explain security issues associated with the solution to management.

Licensed to Berend Post berend.post@it-university.nl

Question 1464

An IS auditor reviewing an organization's data privacy controls observes that privacy notices do not clearly state how the organization uses customer data for its processing operations. Which of the following data protection principles MUST be implemented to address this gap?

- ☐ Maintenance of data integrity
- ☒ Access to collected data
- ☐ Retention of consent documentation
- ☐ Purpose for data collection

Question 1465

Which of the following type of honey pot essentially gives a hacker a real environment to attack?

- ☒ High-interaction
- ☐ Low-interaction
- ☐ Med-interaction
- ☐ None of the choices

Explanation:

Explanation: http://www.ce-infosys.com/english/free_compusec/free_compusec.aspx

High-interaction type of honey pot essentially gives an attacker a real environment to attack.

Also, you should know below information about honey pot for CISA exam:

A Honey pot is a software application that pretends to be an unfortunate server on the internet and is not set up actively protect against break-ins.

There are two types of honey pot:

High-interaction Honey pots – Essentially gives hacker a real environment to attack. High-interaction honey pots imitate the activities of the production systems that host a variety of services and, therefore, an attacker may be allowed a lot of services to waste his time. According to recent research into high-interaction honey pot technology, by employing virtual machines, multiple honey pots can be hosted on a single physical machine. Therefore, even if the honey pot is compromised, it can be restored more quickly. In general, high-interaction honey pots provide more security by being difficult to detect, but they are highly expensive to maintain. If virtual machines are not available, one honey pot must be maintained for each physical computer, which can be exorbitantly expensive. Example: Honey net.

Low interaction – Emulate production environment and therefore, provide more limited information. Low-interaction honey pots simulate only the services frequently requested by attackers. Since they

Licensed to Berend Post berend.post@it-university.nl

consume relatively few resources, multiple virtual machines can easily be hosted on one physical system, the virtual systems have a short response time, and less code is required, reducing the complexity of the virtual system's security. Example: Honeyed.

The following were incorrect answers:

Med-interaction – Not a real type of honey pot

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

http://en.wikipedia.org/wiki/Honeypot_%28computing%29

Question 1466

The objectives of business process improvement should PRIMARILY include:

- ☐ minimal impact on staff
- ☐ incremental changes in productivity
- ☐ changes of organizational boundaries
- ☒ performance optimization

Question 1467

Which of the following is the BEST source of information when assessing the amount of time a project will take?

- ☒ GANTT chart
- ☐ Workforce estimate
- ☐ Critical path analysis
- ☐ Scheduling budget

Licensed to Berend Post berend.post@it-university.nl

Question 1468

How is risk affected if users have direct access to a database at the system level?

- ☐ Risk of unauthorized access increases, but risk of untraceable changes to the database decreases.
- ☒ Risk of unauthorized and untraceable changes to the database increases.
- ☐ Risk of unauthorized access decreases, but risk of untraceable changes to the database increases.
- ☐ Risk of unauthorized and untraceable changes to the database decreases.

Explanation:

Explanation:

If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases.

Question 1469

What is the BEST backup strategy for a large database with data supporting online sales?

- ☒ Weekly full backup with daily incremental backup
- ☐ Daily full backup
- ☐ Clustered servers
- ☐ Mirrored hard disks

Explanation:

Explanation:

Weekly full backup and daily incremental backup is the best backup strategy; it ensures the ability to recover the database and yet reduces the daily backup time requirements. A full backup normally requires a couple of hours, and therefore it can be impractical to conduct a full back up every day. Clustered servers provide a redundant processing capability, but are not a backup.

Mirrored hard disks will not help in case of disaster.

Question 1470

Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

- ☒ End-user involvement
- ☐ Senior management involvement
- ☐ Security administration involvement
- ☐ IS auditing involvement

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

End-user involvement is critical during the business impact assessment phase of business continuity planning.

Question 1471

Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the PRIMARY risk if the new plan is not tested?

- ☒ Catastrophic service interruption
- ☐ High consumption of resources
- ☐ Total cost of the recovery may not be minimized
- ☐ Users and recovery teams may face severe difficulties when activating the plan

Explanation:

Explanation:

Choices B, C and D are all possible problems that might occur, and would cause difficulties and financial losses or waste of resources. However, if a new disaster recovery plan is not tested, the possibility of a catastrophic service interruption is the most critical of all risks.

Question 1472

Calculation of the recovery time objective (RTO) is necessary to determine the:

- ☐ time required to restore files.
- ☐ annual loss expectancy (ALE).
- ☐ point of synchronization.
- ☒ priority of restoration.

Question 1473

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

- ☒ Cold site
- ☐ Hot site
- ☐ Alternate site
- ☐ Warm site

Explanation:

Explanation:

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

Licensed to Berend Post berend.post@it-university.nl

Question 1474

After identifying potential security vulnerabilities, what should be the IS auditor's next step?

- ☐ To evaluate potential countermeasures and compensatory controls
- ☐ To implement effective countermeasures and compensatory controls
- ☒ To perform a business impact analysis of the threats that would exploit the vulnerabilities
- ☐ To immediately advise senior management of the findings

Explanation:

Explanation:

After identifying potential security vulnerabilities, the IS auditor's next step is to perform a business impact analysis of the threats that would exploit the vulnerabilities.

Question 1475

Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

- ☐ Print service, application services
- ☐ Data encryption and compression
- ☐ Dialog management
- ☒ End-to-end connection

Explanation:

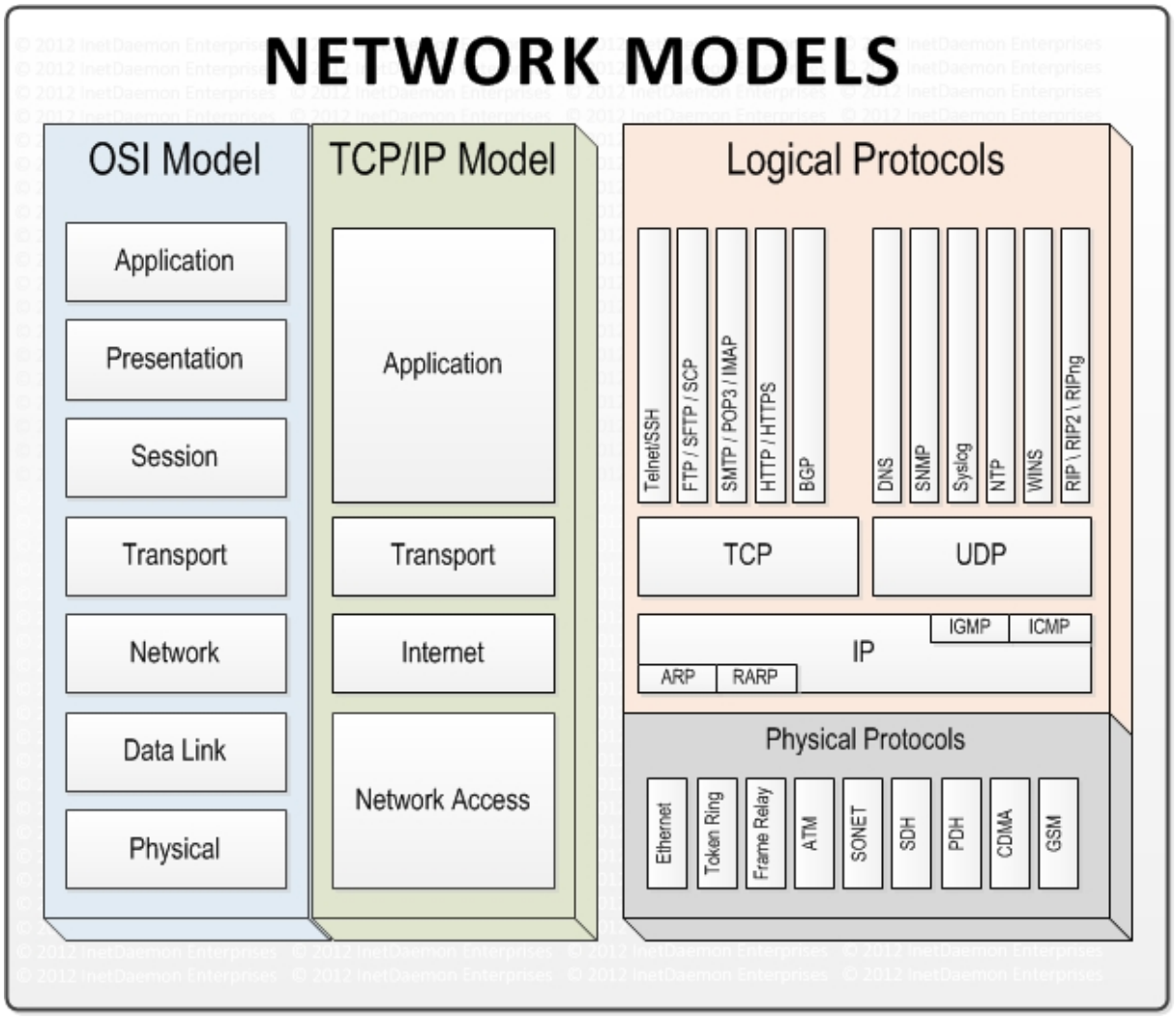
The word NOT is the keyword used in the question. You need to find out a functionality which is not performed by application layer of a TCP/IP model.

End-to-end connection is the Transport layer functionality in TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

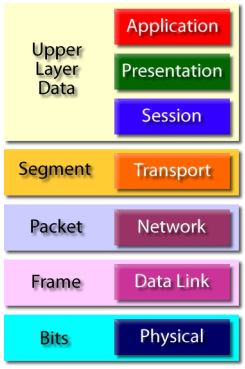
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

The other functionalities described in the options are performed by application layer in TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 1476

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the security manager?

- ☐ Follow the outsourcer's response plan
- ☐ Refer to the organization's response plan
- ☒ Notify the outsourcer of the privacy breach
- ☐ Alert the appropriate law enforcement authorities

Licensed to Berend Post berend.post@it-university.nl

Question 1477

Which of the following is normally a responsibility of the chief security officer (CSO)?

- ☒ Periodically reviewing and evaluating the security policy
- ☐ Executing user application and software testing and evaluation
- ☐ Granting and revoking user access to IT resources
- ☐ Approving access to data and applications

Explanation:

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

Question 1478

An IS audit manager finds that data manipulation logic developed by the audit analytics team leads to incorrect conclusions. This inaccurate logic is MOST likely an indication of which of the following?

- ☐ Incompatibility between data volume and analytics processing capacity.
- ☐ Poor security controls that grant inappropriate access to analysis produced.
- ☒ The team's poor understanding of the business process being analyzed.
- ☐ Poor change controls over data sets collected from the business.

Question 1479

Which of the following is MOST important to ensure when planning a black box penetration test?

- ☐ The test results will be documented and communicated to management.
- ☐ Diagrams of the organization's network architecture are available.
- ☒ The environment and penetration test scope have been determined.
- ☐ The management of the client organization is aware of the testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1480

Which of the following is an estimation technique where the results can be measure by the functional size of an information system based on the number and complexity of input, output, interface and queries?

- ☒ Functional Point analysis
- ☐ Gantt Chart
- ☐ Time box management
- ☐ Critical path methodology

Explanation:

For CISA exam you should know below information about Functional Point Analysis:

Function Point Analysis (FPA) is an ISO recognized method to measure the functional size of an information system. The functional size reflects the amount of functionality that is relevant to and recognized by the user in the business. It is independent of the technology used to implement the system.

The unit of measurement is "function points". So, FPA expresses the functional size of an information system in a number of function points (for example: the size of a system is 314 fop's).

The functional size may be used:

To budget application development or enhancement costs

To budget the annual maintenance costs of the application portfolio

To determine project productivity after completion of the project

To determine the Software Size for cost estimating

All software applications will have numerous elementary processes or independent processes to move data. Transactions (or elementary processes) that bring data from outside the application domain (or application boundary) to inside that application boundary are referred to as external inputs. Transactions (or elementary processes) that take data from a resting position (normally on a file) to outside the application domain (or application boundary) are referred as either an external outputs or external inquiries. Data at rest that is maintained by the application in question is classified as internal logical files. Data at rest that is maintained by another application in question is classified as external interface files.

Types of Function Point Counts:

Development Project Function Point Count

Licensed to Berend Post berend.post@it-university.nl

Function Points can be counted at all phases of a development project from requirements up to and including implementation. This type of count is associated with new development work. Scope creep can be tracked and monitored by understanding the functional size at all phase of a project. Frequently, this type of count is called a baseline function point count.

Enhancement Project Function Point Count

It is common to enhance software after it has been placed into production. This type of function point count tries to size enhancement projects. All production applications evolve over time. By tracking enhancement size and associated costs a historical database for your organization can be built. Additionally, it is important to understand how a Development project has changed over time.

Application Function Point Count

Application counts are done on existing production applications. This “baseline count” can be used with overall application metrics like total maintenance hours. This metric can be used to track maintenance hours per function point. This is an example of a normalized metric. It is not enough to examine only maintenance, but one must examine the ratio of maintenance hours to size of the application to get a true picture.

Productivity:

The definition of productivity is the output-input ratio within a time period with due consideration for quality.

Productivity = outputs/inputs (within a time period, quality considered)

The formula indicates that productivity can be improved by (1) by increasing outputs with the same inputs, (2) by decreasing inputs but maintaining the same outputs, or (3) by increasing outputs and decreasing inputs change the ratio favorably.

Software Productivity = Function Points / Inputs

Effectiveness vs. Efficiency:

Productivity implies effectiveness and efficiency in individual and organizational performance. Effectiveness is the achievement of objectives. Efficiency is the achievement of the ends with least amount of resources.

Software productivity is defined as hours/function points or function points/hours. This is the average cost to develop software or the unit cost of software. One thing to keep in mind is the unit

Licensed to Berend Post berend.post@it-university.nl

cost of software is not fixed with size. What industry data shows is the unit cost of software goes up with size.

Average cost is the total cost of producing a particular quantity of output divided by that quantity. In this case to Total Cost/Function Points. Marginal cost is the change in total cost attributable to a one-unit change in output.

There are a variety of reasons why marginal costs for software increase as size increases. The following is a list of some of the reasons

As size becomes larger complexity increases.

As size becomes larger a greater number of tasks need to be completed.

As size becomes larger there is a greater number of staff members and they become more difficult to manage.

Function Points are the output of the software development process. Function points are the unit of software. It is very important to understand that Function Points remain constant regardless who develops the software or what language the software is developed in. Unit costs need to be examined very closely. To calculate average unit cost all items (units) are combined and divided by the total cost. On the other hand, to accurately estimate the cost of an application each component cost needs to be estimated.

Determine type of function point count

Determine the application boundary

Identify and rate transactional function types to determine their contribution to the unadjusted function point count.

Identify and rate data function types to determine their contribution to the unadjusted function point count.

Determine the value adjustment factor (VAF)

Calculate the adjusted function point count.

To complete a function point count knowledge of function point rules and application documentation is needed. Access to an application expert can improve the quality of the count. Once the application boundary has been established, FPA can be broken into three major parts

Licensed to Berend Post berend.post@it-university.nl

FPA for transactional function types

FPA for data function types

FPA for GSCs

Rating of transactions is dependent on both information contained in the transactions and the number of files referenced, it is recommended that transactions are counted first. At the same time a tally should be kept of all FTR's (file types referenced) that the transactions reference. Every FTR must have at least one or more transactions. Each transaction must be an elementary process. An elementary process is the smallest unit of activity that is meaningful to the end user in the business. It must be self-contained and leave the business in consistent state

The following were incorrect answers:

Critical Path Methodology - The critical path method (CPM) is an algorithm for scheduling a set of project activities

Gantt Chart - A Gantt chart is a type of bar chart, developed by Henry Gantt in the 1910s, that illustrates a project schedule. Gantt charts illustrate the start and finish dates of the terminal elements and summary elements of a project. Terminal elements and summary elements comprise the work breakdown structure of the project. Modern Gantt charts also show the dependency (i.e. precedence network) relationships between activities. Gantt charts can be used to show current schedule status using percent-complete shadings and a vertical "TODAY" line as shown here.

Time box Management - In time management, a time boxing allocates a fixed time period, called a time box, to each planned activity. Several project management approaches use time boxing. It is also used for individual use to address personal tasks in a smaller time frame. It often involves having deliverables and deadlines, which will improve the productivity of the user.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 154

Licensed to Berend Post berend.post@it-university.nl

Question 1481

Which of the following should be seen as one of the most significant factors considered when determining the frequency of IS audits within your organization?

- ☐ The cost of risk analysis
- ☐ The income generated by the business function
- ☐ Resource allocation strategy
- ☒ The nature and level of risk
- ☐ None of the choices.

Explanation:

Explanation:

You use a risk assessment process to describe and analyze the potential audit risks inherent in a given line of business. You should update such risk assessment at least annually to reflect changes. The level and nature of risk should be the most significant factors to be considered when determining the frequency of audits.

Question 1482

An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:

- ☐ accept the DBA access as a common practice.
- ☒ assess the controls relevant to the DBA function.
- ☐ recommend the immediate revocation of the DBA access to production data.
- ☐ review user access authorizations approved by the DBA.

Explanation:

Explanation:

It is good practice when finding a potential exposure to look for the best controls. Though granting the database administrator (DBA) access to production data might be a common practice, the IS auditor should evaluate the relevant controls. The DBA should have access based on a need-to- know and need-to-do basis; therefore, revocation may remove the access required. The DBA, typically, may need to have access to some production data. Granting user authorizations is the responsibility of the data owner and not the DBA.

Question 1483

Which of the following security testing techniques is MOST effective in discovering unknown malicious attacks?

- ☐ Vulnerability testing
- ☐ Reverse engineering
- ☒ Penetration testing
- ☐ Sandboxing

Licensed to Berend Post berend.post@it-university.nl

Question 1484

Who is accountable for maintaining appropriate security measures over information assets?

- ☒ Data and systems owners
- ☐ Data and systems users
- ☐ Data and systems custodians
- ☐ Data and systems auditors

Explanation:

Explanation:

Data and systems owners are accountable for maintaining appropriate security measures over information assets.

Question 1485

Which of the following is MOST useful to include in a report to senior management on a regular basis to demonstrate the effectiveness of the information security program?

- ☐ Critical success factors (CSFs)
- ☐ Key risk indicators (KRIs)
- ☐ Capability maturity models
- ☒ Key performance indicators (KPIs)

Question 1486

The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan (DRP)?

- ☒ Contact information of key personnel
- ☐ Server inventory documentation
- ☐ individual roles and responsibilities
- ☐ Procedures for declaring a disaster

Explanation:

Explanation:

In the event of a disaster, it is important to have a current updated list of personnel who are key to the operation of the plan. Choices B, C and D would be more likely to remain stable overtime.

Licensed to Berend Post berend.post@it-university.nl

Question 1487

Which of the following is MOST likely to be included in an enterprise information security policy?

- ☐ Password composition requirements
- ☒ Consequences of noncompliance
- ☐ Audit trail review requirements
- ☐ Security monitoring strategy

Question 1488

The PRIMARY advantage of object-oriented technology is enhanced:

- ☐ efficiency due to the re-use of elements of logic.
- ☐ management of sequential program execution for data access.
- ☐ management of a restricted variety of data types for a data object.
- ☒ grouping of objects into methods for data access.

Question 1489

Which of the following cloud computing service model provides a way to rent operating systems, storage and network capacity over the Internet?

- ☐ Software as a service
- ☐ Data as a service
- ☒ Platform as a service
- ☐ Infrastructure as a service

Explanation:

Platform as a Service (Peas) is a way to rent operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

For your exam you should know below information about Cloud Computing:

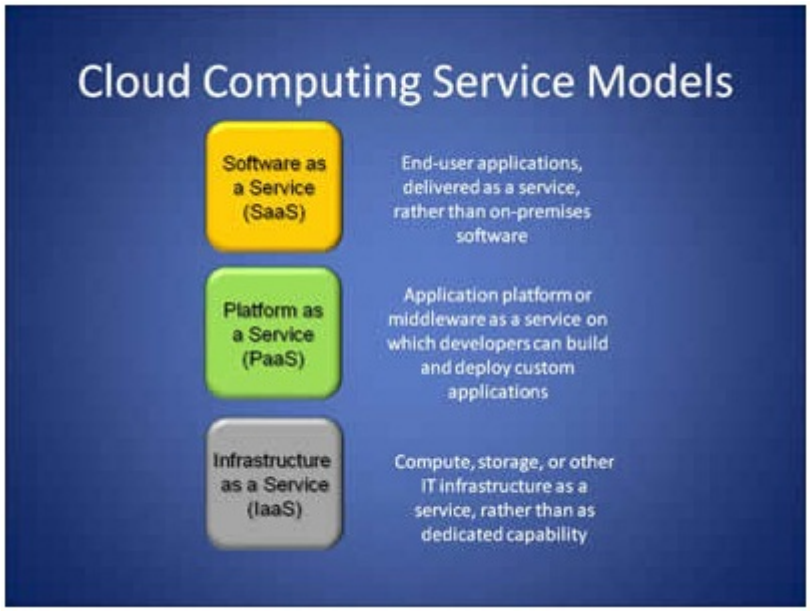
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing

Cloud computing service models:

Licensed to Berend Post berend.post@it-university.nl

Cloud computing service models



Software as a Service (Seas)

Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for Seas. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for Seas distribution.

Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for Seas distribution and use.

Benefits of the Seas model include:

easier administration

automatic updates and patch management

compatibility: All users will have the same version of software.

easier collaboration, for the same reason

global accessibility.

Licensed to Berend Post berend.post@it-university.nl

Platform as a Service (Peas)

Platform as a Service (Peas) is a way to rent operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Where Iasi is the “raw IT network,” Peas is the software environment that runs on top of the IT network.

Platform as a Service (Peas) is an outgrowth of Software as a Service (Seas), a software distribution model in which hosted software applications are made available to customers over the Internet. Peas has several advantages for developers. With Peas, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

On the downside, Peas involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

Infrastructure as a Service (Iasi)

Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Characteristics and components of Iasi include:

Utility computing service and billing model.

Automation of administrative tasks.

Dynamic scaling.

Licensed to Berend Post berend.post@it-university.nl

Desktop virtualization.

Policy-based services.

Internet connectivity.

Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.

Software as a service - Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. Seas is closely related to the ASP (application service provider) and on demand computing software delivery models.

Infrastructure as a service - Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689

http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

Licensed to Berend Post berend.post@it-university.nl

Question 1490

Following a malicious security incident, an organization has decided to prosecute those responsible. Which of the following will BEST facilitate the forensic investigation?

- ☐ Identifying the affected environment
- ☐ Performing a backup of affected systems
- ☐ Determining the degree of loss
- ☒ Maintaining chain of custody

Question 1491

Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☒ Error Rate

Explanation:

Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched

Licensed to Berend Post berend.post@it-university.nl

network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 275

Question 1492

Which of the following controls will BEST ensure that the board of directors receives sufficient information about IT?

- ☐ The CIO reports on performance and corrective actions in a timely manner.
- ☐ Regular meetings occur between the board, the CIO. and a technology committee.
- ☐ The CIO regularly sends IT trend reports to the board.
- ☒ Board members are knowledgeable about IT, and the CIO is consulted on IT issues.

Licensed to Berend Post berend.post@it-university.nl

Question 1493

Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

- ☐ 128-bit wired equivalent privacy (WEP)
- ☐ MAC-based pre-shared key(PSK)
- ☒ Randomly generated pre-shared key (PSKJ
- ☐ Alphanumeric service set identifier (SSID)

Explanation:

Explanation:

A randomly generated PSK is stronger than a MAC-based PSK, because the MAC address of a computer is fixed and often accessible. WEP has been shown to be a very weak encryption technique and can be cracked within minutes. The SSID is broadcast on the wireless network in plaintext.

Question 1494

When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

When participating in a systems-development project, an IS auditor should also strive to ensure that adequate and complete documentation exists for all projects.

Question 1495

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

- ☒ Statistical-based
- ☐ Signature-based
- ☐ Neural network
- ☐ Host-based

Explanation:

Explanation:

A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. A neural network combines the previous

Licensed to Berend Post berend.post@it-university.nl

two IDSs to create a hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be host- or network-based.

Question 1496

An IS auditor finds that intellectual property is not being protected to the level specified in the organization's data classification and protection policy. The business owner is aware of this issue and chooses to accept the risk. Which of the following is the auditor's BEST course of action?

- ☒ Note the finding and request formal acceptance.
- ☐ Include the finding in the follow-up audit.
- ☐ Amend the data classification policy.
- ☐ Form a committee and further investigate the issue.

Question 1497

What is the primary security concern for EDI environments?

- ☐ Transaction authentication
- ☐ Transaction completeness
- ☐ Transaction accuracy
- ☒ Transaction authorization

Explanation:

Explanation: Transaction authorization is the primary security concern for EDI environments.

Question 1498

When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

- ☐ implement controls to mitigate the risk.
- ☐ report compliance to management.
- ☒ review the residual risk level.
- ☐ monitor for business changes.

Question 1499

Which of the following IT governance best practices improves strategic alignment?

- ☐ Supplier and partner risks are managed.
- ☐ A knowledge base on customers, products, markets and processes is in place.
- ☐ A structure is provided that facilitates the creation and sharing of business information.
- ☒ Top management mediate between the imperatives of business and technology.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management.

Question 1500

Which of the following should an IS auditor expect to see in a network vulnerability assessment?

- ☐ Misconfiguration and missing updates
- ☐ Malicious software and spyware
- ☒ Security design flaws
- ☐ Zero-day vulnerabilities

Question 1501

Which of the following is a good control for protecting confidential data residing on a PC?

- ☐ Personal firewall
- ☐ File encapsulation
- ☒ File encryption
- ☐ Host-based intrusion detection

Explanation:

Explanation:

File encryption is a good control for protecting confidential data residing on a PC.

Question 1502

A database administrator should be prevented from:

- ☐ using an emergency user ID.
- ☒ accessing sensitive information.
- ☐ having end user responsibilities.
- ☐ having access to production files.

Licensed to Berend Post berend.post@it-university.nl

Question 1503

An airline's online booking system uses an automated script that checks whether fares are within the defined threshold of what is reasonable before the fares are displayed on the website. Which type of control is in place?

- ☐ Compensating control
- ☐ Preventive control
- ☒ Detective control
- ☐ Corrective control

Question 1504

Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

- ☐ Targeted testing
- ☐ External testing
- ☐ internal testing
- ☒ Double-blind testing

Explanation:

Explanation:

In a double-blind test, the administrator and security staff are not aware of the test, which will result in an assessment of the incident handling and response capability in an organization. In targeted, external, and internal testing, the system administrator and security staff are aware of the tests since they are informed before the start of the tests.

Question 1505

During the implementation of a new system, an IS auditor must assess whether certain automated calculations comply with the regulatory requirements. Which of the following is the BEST way to obtain this assurance?

- ☐ Inspect user acceptance test results.
- ☒ Re-perform the calculation with audit software.
- ☐ Review sign-off documentation.
- ☐ Review the source code related to the calculation.

Licensed to Berend Post berend.post@it-university.nl

Question 1506

An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

- ☐ Digitalized signatures
- ☐ Hashing
- ☐ Parsing
- ☒ Steganography

Explanation:

Explanation:

Steganography is a technique for concealing the existence of messages or information. An increasingly important stenographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes, and is widely applied in the design of programming languages or in data entry editing.

Question 1507

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

With the objective of mitigating the risk and impact of a major business interruption, a disaster-recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

Licensed to Berend Post berend.post@it-university.nl

Question 1508

Which cloud deployment model is MOST likely to be limited in scalability?

- ☐ Public
- ☒ Private
- ☐ Hybrid
- ☐ Community

Question 1509

An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

- ☐ That an audit clause is present in all contracts
- ☐ That the SLA of each contract is substantiated by appropriate KPIs
- ☒ That the contractual warranties of the providers support the business needs of the organization
- ☐ That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Explanation:

Explanation:

The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

Question 1510

Which of the following attack involves slicing small amount of money from a computerize transaction or account?

- ☐ Eavesdropping
- ☐ Traffic Analysis
- ☒ Salami
- ☐ Masquerading

Explanation:

Salami slicing or Salami attack refers to a series of many small actions, often performed by clandestine means, that as an accumulated whole produces a much larger action or result that would be difficult or unlawful to perform all at once. The term is typically used pejoratively. Although salami slicing is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well.

An example of salami slicing, also known as penny shaving, is the fraudulent practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to the

Licensed to Berend Post berend.post@it-university.nl

nearest cent (or other monetary unit) in financial transactions. It would be done by always rounding down, and putting the fractions of a cent into another account. The idea is to make the change small enough that any single transaction will go undetected.

In information security, a salami attack is a series of minor attacks that together results in a larger attack. Computers are ideally suited to automating this type of attack.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they’ve gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

The following reference(s) were/was used to create this question:

http://searchfinancialsecurity.techtarget.com/definition/eavesdropping

http://en.wikipedia.org/wiki/Salami_slicing

Licensed to Berend Post berend.post@it-university.nl

http://en.wikipedia.org/wiki/Eavesdropping

http://en.wikipedia.org/wiki/Traffic_analysis

http://www.techopedia.com/definition/4020/masquerade-attack

Question 1511

Which of the following is the PRIMARY benefit of including IT management and staff when conducting control self-assessments (CSAs) within an organization?

- ☒ It helps to identify risk to the business.
- ☐ It improves the efficiency of business and IT operational processes.
- ☐ It increases buy-in for more stringent controls.
- ☐ It reduces the workload of external and internal auditors.

Question 1512

The risks associated with electronic evidence gathering would MOST likely be reduced by an e- mail:

- ☐ destruction policy.
- ☐ security policy.
- ☒ archive policy.
- ☐ audit policy.

Explanation:

Explanation:

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

Question 1513

During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor's BEST course of action?

- ☐ Adjust the annual risk assessment accordingly.
- ☐ Require the auditee to address the recommendations in full.
- ☒ Evaluate senior management's acceptance of the risk.
- ☐ Update the audit program based on management's acceptance of risk.

Licensed to Berend Post berend.post@it-university.nl

Question 1514

An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?

- ☐ User-level permissions
- ☒ Role-based
- ☐ Fine-grained
- ☐ Discretionary

Explanation:

Explanation:

Role-based access controls the system access by defining roles for a group of users. Users are assigned to the various roles and the access is granted based on the user's role. User-level permissions for an ERP system would create a larger administrative overhead. Fine-grained access control is very difficult to implement and maintain in the context of a large enterprise.

Discretionary access control may be configured or modified by the users or data owners, and therefore may create inconsistencies in the access control management.

Question 1515

The PRIMARY purpose of an IT forensic audit is:

- ☐ to participate in investigations related to corporate fraud.
- ☒ the systematic collection of evidence after a system irregularity.
- ☐ to assess the correctness of an organization's financial statements
- ☐ to determine that there has been criminal activity.

Explanation:

Explanation:

Choice B describes a forensic audit. The evidence collected could then be used in judicial proceedings. Forensic audits are not limited to corporate fraud. Assessing the correctness of an organization’s financial statements is not the purpose of a forensic audit. Drawing a conclusion to criminal activity would be part of a legal process and not the objective of a forensic audit.

Question 1516

Which of the following tasks should be performed during an organization’s business continuity plan (BCP) test?

- ☐ Evaluate the security at the offsite facility.
- ☐ Review the coverage of insurance.
- ☒ Assess the critical information retrieval capability.
- ☐ Review the alternate processing site contract.

Licensed to Berend Post berend.post@it-university.nl

Question 1517

Which of the following is the most fundamental step in preventing virus attacks?

- ☒ Adopting and communicating a comprehensive antivirus policy
- ☐ Implementing antivirus protection software on users' desktop computers
- ☐ Implementing antivirus content checking at all network-to-Internet gateways
- ☐ Inoculating systems with antivirus code

Explanation:

Explanation:

Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

Question 1518

Which of the following factors will BEST promote effective information security management?

- ☒ Senior management commitment
- ☐ Identification and risk assessment of sensitive resources
- ☐ Security awareness training
- ☐ Security policy framework

Question 1519

During a computer forensics investigation, what is the PRIMARY reason for obtaining a bit-for-bit copy of data in storage?

- ☐ To document findings
- ☒ To obtain residual data
- ☐ To obtain data as well as source code details
- ☐ To transfer the data into a controlled location

Question 1520

Which of the following attack is against computer network and involves fragmented or invalid ICMP packets sent to the target?

- ☒ Nuke attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Explanation:

A Nuke attack is an old denial-of-service attack against computer networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to

Licensed to Berend Post berend.post@it-university.nl

repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.

A specific example of a nuke attack that gained some prominence is the Win Nuke, which exploited the vulnerability in the NetBIOS handler in Windows 95. A string of out-of-band data was sent to TCP port 139 of the victim's machine, causing it to lock up and display a Blue Screen of Death (BSOD).

The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 322

Question 1521

A disk management system's PRIMARY function is to:

- ☐ monitor disk accesses for analytical review
- ☐ deny access to disk resident data files
- ☐ provide data on efficient disk usage
- ☒ provide the method of control for disk usage

Licensed to Berend Post berend.post@it-university.nl

Question 1522

Which of the following provides the strongest authentication for physical access control?

- ☐ Sign-in logs
- ☐ Dynamic passwords
- ☐ Key verification
- ☒ Biometrics

Explanation:

Explanation:

Biometrics can be used to provide excellent physical access control.

Question 1523

Which of the following is the MOST critical characteristic of a biometric system?

- ☐ Registration time
- ☐ Throughput rate
- ☒ Accuracy
- ☐ Ease of use

Question 1524

A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

- ☐ Deletion
- ☒ Input
- ☐ Access
- ☐ Duplication

Explanation:

Explanation:

A transaction journal provides the information necessary for detecting unauthorized input from a terminal.

Question 1525

When protecting the confidentiality of information assets, the MOST effective control practice is the:

- ☐ awareness training of personnel on regulatory requirements.
- ☐ enforcement of a need-to-know access control philosophy.
- ☒ utilization of a dual-factor authentication mechanism.
- ☐ configuration of read-only access to all users.

Licensed to Berend Post berend.post@it-university.nl

Question 1526

A system administrator recently informed the IS auditor about the occurrence of several unsuccessful intrusion attempts from outside the organization. Which of the following is MOST effective in detecting such an intrusion?

- ☐ Installing biometrics-based authentication
- ☐ Configuring the router as a firewall
- ☒ Periodically reviewing log files
- ☐ Using smart cards with one-time passwords

Question 1527

Which of the following cloud deployment models would BEST meet the needs of a startup software development organization with limited initial capital?

- ☐ Private
- ☒ Public
- ☐ Community
- ☐ Hybrid

Question 1528

The MOSTimportant objective of security awareness training for business staff is to:

- ☐ understand intrusion methods
- ☐ reduce negative audit findings
- ☐ increase compliance
- ☒ modify behavior

Question 1529

An IS auditor has discovered that a cloud-based application was not included in an application inventory that was used to confirm the scope of an audit. The business process owner explained that the application will be audited by a third party in the next year. The auditor's NEXT step should be to:

- ☐ evaluate the impact of the cloud application on the audit scope
- ☐ revise the audit scope to include the cloud-based application
- ☐ review the audit report when performed by the third party
- ☒ report the control deficiency to senior management

Licensed to Berend Post berend.post@it-university.nl

Question 1530

The PRIMARY purpose of a security information and event management (SIEM) system is to:

- ☒ identify potential incidents
- ☐ provide status of incidents
- ☐ resolve incidents
- ☐ track ongoing incidents

Question 1531

Which of the following is a mechanism for mitigating risks?

- ☒ Security and control practices
- ☐ Property and liability insurance
- ☐ Audit and certification
- ☐ Contracts and service level agreements (SLAs)

Explanation:

Explanation:

Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, while contracts and SLAs are mechanisms of risk allocation.

Question 1532

Which of the following is the BEST course of action for an information security manager to align security and business goals?

- ☐ Reviewing the business strategy
- ☐ Actively engaging with stakeholders
- ☐ Conducting a business impact analysis
- ☒ Defining key performance indicators

Question 1533

A disaster recovery plan for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

- ☐ A hot site that can be operational in eight hours with asynchronous backup of the transaction logs
- ☐ Distributed database systems in multiple locations updated asynchronously
- ☐ Synchronous updates of the data and standby active systems in a hot site
- ☒ Synchronous remote copy of the data in a warm site that can be operational in 48 hours

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The synchronous copy of the storage achieves the RPO objective and a warm site operational in 48 hours meets the required RTO. Asynchronous updates of the database in distributed locations do not meet the RPO. Synchronous updates of the data and standby active systems in a hot site meet the RPO and RTO requirements but are more costly than a warm site solution.

Question 1534

An organization plans to launch a social media presence as part of a new customer service campaign. Which of the following is the MOST significant risk from the perspective of potential litigation?

- ☒ The policy stating what employees can post on the organization's behalf is unclear.
- ☐ Access to corporate-sponsored social media accounts requires only single-factor authentication.
- ☐ Approved employees can use personal devices to post on the company's behalf.
- ☐ There is a lack of clear procedures for responding to customers on social media outlets.

Question 1535

When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

- ☐ recommend that the database be normalized.
- ☐ review the conceptual data model.
- ☐ review the stored procedures.
- ☒ review the justification.

Explanation:

Explanation:

If the database is not normalized, the IS auditor should review the justification since, in some situations, denormalization is recommended for performance reasons. The IS auditor should not recommend normalizing the database until further investigation takes place. Reviewing the conceptual data model or the stored procedures will not provide information about normalization.

Question 1536

What is the MOST effective method of preventing unauthorized use of data files?

- ☐ Automated file entry
- ☐ Tape librarian
- ☒ Access control software
- ☐ Locked library

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Access control software is an active control designed to prevent unauthorized access to data.

Question 1537

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

- ☐ Cold-site facilities
- ☐ Disaster recovery for networks
- ☐ Diverse processing
- ☒ Disaster recovery for systems

Explanation:

Explanation:

Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

Question 1538

Which of the following is the GREATEST risk when implementing a data warehouse?

- ☐ increased response time on the production systems
- ☒ Access controls that are not adequate to prevent data modification
- ☐ Data duplication
- ☐ Data that is not updated or current

Explanation:

Explanation:

Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production data. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

Question 1539

An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

- ☐ hardware configuration.
- ☐ access control software.
- ☒ ownership of intellectual property.
- ☐ application development methodology.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

Question 1540

Which of the following BEST supports the prioritization of new IT projects?

- ☐ Internal control self-assessment (CSA)
- ☐ Information systems audit
- ☒ Investment portfolio analysis
- ☐ Business risk assessment

Explanation:

Explanation:

It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal control self-assessment (CSA) may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects.

Business risk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

Question 1541

The MAIN reason an organization's incident management procedures should include a post-incident review is to:

- ☐ ensure evidence is collected for possible post-event litigation.
- ☐ take appropriate action when procedures are not followed.
- ☐ enable better reporting for executives and the audit committee.
- ☒ improve processes by learning from identified weaknesses.

Licensed to Berend Post berend.post@it-university.nl

Question 1542

During a follow-up audit, an IS auditor discovers that a recommendation has not been implemented. However, the auditee has implemented a manual workaround that addresses the identified risk, through far less efficiency than the recommended action would. Which of the following would be the auditor's BEST course of action?

- ☐ Notify management that the risk has been addressed and take no further action.
- ☐ Escalate the remaining issue for further discussion and resolution.
- ☒ Note that the risk has been addressed and notify management of the inefficiency.
- ☐ Insist to management that the original recommendation be implemented.

Question 1543

The MAJOR reason for segregating test programs from production programs is to:

- ☐ achieve segregation of duties between IS staff and end users.
- ☐ limit access rights of IS staff to the development environment.
- ☐ provide control over program changes.
- ☒ provide the basis for efficient system change management.

Question 1544

Which of the following would contribute MOST to employees' understanding of data handling responsibilities?

- ☐ Requiring staff acknowledgement of security policies
- ☐ Labeling documents according to appropriate security classification
- ☒ Implementing a tailored security awareness training program
- ☐ Demonstrating support by senior management of the security program

Question 1545

In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

- ☒ common gateway interface (CGI) scripts.
- ☐ enterprise Java beans (EJBs).
- ☐ applets.
- ☐ web services.

Explanation:

Explanation: Common gateway interface (CGI) scripts are executable machine independent software programs on the server that can be called and executed by a web server page. CGI performs specific tasks such as processing inputs received from clients. The use of CGI scripts needs to be evaluated, because as they run in the server, a bug in them may allow a user to gain unauthorized access to the server and from there gain access to the organization's network.

Licensed to Berend Post berend.post@it-university.nl

Applets are programs downloaded from a web server and executed on web browsers on client machines to run any web-based applications. Enterprise java beans (EJBs) and web services have to be deployed by the web server administrator and are controlled by the application server. Their execution requires knowledge of the parameters and expected return values.

Question 1546

Which of the following is an example of the defense in-depth security principle?

- ☐ Using two firewalls of different vendors to consecutively check the incoming network traffic
- ☒ Using a firewall as well as logical access controls on the hosts to control incoming network traffic
- ☐ Having no physical signs on the outside of a computer center building
- ☐ Using two firewalls in parallel to check different types of incoming traffic

Explanation:

Explanation:

Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

Question 1547

Which of the following attack redirects outgoing message from the client back onto the client, preventing outside access as well as flooding the client with the sent packets?

- ☒ Banana attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Explanation:

A "banana attack" is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets.

The Banana attack uses a router to change the destination address of a frame. In the Banana attack:

Licensed to Berend Post berend.post@it-university.nl

A compromised router copies the source address on an inbound frame into the destination address.

The outbound frame bounces back to the sender.

This sender is flooded with frames and consumes so many resources that valid service requests can no longer be processed.

The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 321

Question 1548

An organization uses two data centers. Which of the following would BEST address the organization's need for high resiliency?

- ☒ The data centers act as mirrored sites.
- ☐ Each data center is recoverable via tape backups.
- ☐ A hot site is used for the second site.
- ☐ There is data replication across the data centers.

Licensed to Berend Post berend.post@it-university.nl

Question 1549

Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

- ☐ Reviewing a report of security rights in the system
- ☐ Reviewing the complexities of authorization objects
- ☒ Building a program to identify conflicts in authorization
- ☐ Examining recent access rights violation cases

Explanation:

Explanation:

Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. A program could be developed to identify these conflicts. A report of security rights in the enterprise resource planning (ERP) system would be voluminous and time consuming to review; therefore, this technique is not as effective as building a program. As complexities increase, it becomes more difficult to verify the effectiveness of the systems and complexity is not, in itself, a link to segregation of duties. It is good practice to review recent access rights violation cases; however, it may require a significant amount of time to truly identify which violations actually resulted from an inappropriate segregation of duties.

Question 1550

Which of the following is often used as a detection and deterrent control against Internet attacks?

- ☒ Honeypots
- ☐ CCTV
- ☐ VPN
- ☐ VLAN

Explanation:

Explanation:

Honeypots are often used as a detection and deterrent control against Internet attacks.

Question 1551

Reevaluation of risk is MOST critical when there is:

- ☐ resistance to the implementation of mitigating controls
- ☐ a change in security policy
- ☐ a management request for updated security reports
- ☒ a change in the threat landscape

Licensed to Berend Post berend.post@it-university.nl

Question 1552

An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

- ☒ False-acceptance rate (FAR)
- ☐ Equal-error rate (EER)
- ☐ False-rejection rate (FRR)
- ☐ False-identification rate (FIR)

Explanation:

Explanation:

FAR is the frequency of accepting an unauthorized person as authorized, thereby granting access when it should be denied, in an organization with high security requirements, user annoyance with a higher FRR is less important, since it is better to deny access to an authorized individual than to grant access to an unauthorized individual. EER is the point where the FAR equals the FRR; therefore, it does not minimize the FAR. FIR is the probability that an authorized person is identified, but is assigned a false ID.

Question 1553

How does the digital envelop work? What are the correct steps to follow?

- ☐ You encrypt the data using a session key and then encrypt session key using private key of a sender
- ☐ You encrypt the data using the session key and then you encrypt the session key using sender's public key
- ☒ You encrypt the data using the session key and then you encrypt the session key using the receiver's public key
- ☐ You encrypt the data using the session key and then you encrypt the session key using the receiver's private key

Explanation:

The process of encrypting bulk data using symmetric key cryptography and then encrypting the session key using public key algorithm is referred as a digital envelope.

A Digital Envelope is used to send encrypted information using symmetric crypto cipher and then key session along with it. It is secure method to send electronic document without compromising the data integrity, authentication and non-repudiation, which were obtained with the use of symmetric keys.

A Digital envelope mechanism works as follows:

The symmetric key used to encrypt the message can be referred to as session key. The bulk of the message would take advantage of the high speed provided by Symmetric Cipher.

Licensed to Berend Post berend.post@it-university.nl

The session key must then be communicated to the receiver in a secure way to allow the receiver to decrypt the message.

If the session key is sent to receiver in the plain text, it could be captured in clear text over the network and anyone could access the session key which would lead to confidentiality being compromised.

Therefore it is critical to encrypt the session key with the receiver public key before sending it to the receiver. The receiver's will use their matching private key to decrypt the session key which then allow them to decrypt the message using the session key.

The encrypted message and the encrypted session key are sent to the receiver who, in turn decrypts the session key with the receiver's private key. The session key is then applied to the message cipher text to get the plain text.

The following were incorrect answers:

You encrypt the data using a session key and then encrypt session key using private key of a sender - If the session key is encrypted using sender's private key, it can be decrypted only using sender's public key. The sender's public key is known to everyone so anyone can decrypt session key and message.

You encrypt the data using the session key and then you encrypt the session key using sender's public key - If the session key is encrypted by using sender's public key then only sender can decrypt the session key using his/her own private key and receiver will not be able to decrypt the same.

You encrypt the data using the session key and then you encrypt the session key using the receiver's private key - Sender should not have access to receiver's private key. This is not a valid option.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 350 and 351

Question 1554

In an EDI process, the device which transmits and receives electronic documents is the:

- ☒ communications handler.
- ☐ EDI translator.
- ☐ application interface.
- ☐ EDI interface.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

Question 1555

Of the following, who should the security manager consult FIRST when determining the severity level of a security incident involving a third-party vendor?

- ☐ IT process owners
- ☒ Business partners
- ☐ Risk manager
- ☐ Business process owners

Question 1556

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

- ☐ The project budget
- ☒ The critical path for the project
- ☐ The length of the remaining tasks
- ☐ The personnel assigned to other tasks

Explanation:

Explanation:

Since adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will in fact shorten the project duration. Given that there may be slack time available on some of the other tasks not on the critical path, factors such as the project budget, the length of other tasks and the personnel assigned to them may or may not be affected.

Question 1557

When assessing a business case as part of a post-implementation review, the IS auditor must ensure that the:

- ☐ feasibility of alternative project approaches has been assessed.
- ☐ business case has not been amended since project approval.
- ☐ quality assurance measures have been applied throughout the project.
- ☒ amendments to the business case have been approved.

Licensed to Berend Post berend.post@it-university.nl

Question 1558

An IS audit report highlighting inadequate network internal controls is challenged because no serious incident has ever occurred. Which of the following actions performed during the audit would have BEST supported the findings?

- ☐ Compliance testing
- ☐ Threat risk assessment
- ☒ Penetration testing
- ☐ Vulnerability assessment

Question 1559

During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

- ☒ enrollment.
- ☐ identification.
- ☐ verification.
- ☐ storage.

Explanation:

Explanation:

The users of a biometrics device must first be enrolled in the device. The device captures a physical or behavioral image of the human, identifies the unique features and uses an algorithm to convert them into a string of numbers stored as a template to be used in the matching processes.

Question 1560

A vendor service level agreement (SLA) requires backups to be physically secured. An IS audit of the backup system revealed a number of the backup media were missing. Which of the following should be the auditor's NEXT step?

- ☐ Recommend a review of the vendor's contract.
- ☒ Recommend identification of the data stored on the missing media.
- ☐ Notify executive management.
- ☐ Include the missing backup media finding in the audit report.

Question 1561

Which of the following should be of MOST concern to an IS auditor?

- ☒ Lack of reporting of a successful attack on the network
- ☐ Failure to notify police of an attempted intrusion
- ☐ Lack of periodic examination of access rights
- ☐ Lack of notification to the public of an intrusion

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Not reporting an intrusion is equivalent to an IS auditor hiding a malicious intrusion, which would be a professional mistake. Although notification to the police may be required and the lack of a periodic examination of access rights might be a concern, they do not represent as big a concern as the failure to report the attack. Reporting to the public is not a requirement and is dependent on the organization's desire, or lack thereof, to make the intrusion known.

Question 1562

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- ☒ System owners
- ☐ System users
- ☐ System designers
- ☐ System builders

Explanation:

Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system.

Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

Question 1563

An organization has purchased a security information and event management (SIEM) tool. Which of the following would be MOST important to consider before implementation?

- ☐ The contract with the SIEM vendor
- ☒ Controls to be monitored
- ☐ Available technical support
- ☐ Reporting capabilities

Question 1564

The rate of change in technology increases the importance of:

- ☐ outsourcing the IS function.
- ☒ implementing and enforcing good processes.
- ☐ hiring personnel willing to make a career within the organization.
- ☐ meeting user requirements.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

Question 1565

During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

- ☐ an unauthorized user may use the ID to gain access.
- ☐ user access management is time consuming.
- ☐ passwords are easily guessed.
- ☒ user accountability may not be established.

Explanation:

Explanation:

The use of a single user ID by more than one individual precludes knowing who in fact used that ID to access a system; therefore, it is literally impossible to hold anyone accountable. All user IDs, not just shared IDs, can be used by unauthorized individuals. Access management would not be any different with shared IDs, and shared user IDs do not necessarily have easily guessed passwords.

Question 1566

Which of the following would present the GREATEST need to revise information security policies?

- ☐ An increase in reported incidents
- ☒ A merger with a competing company
- ☐ Implementation of a new firewall
- ☐ Changes in standards and procedures

Question 1567

The prioritization of incident response actions should be PRIMARILY based on which of the following?

- ☐ Scope of disaster
- ☒ Business impact
- ☐ Availability of personnel
- ☐ Escalation process

Licensed to Berend Post berend.post@it-university.nl

Question 1568

Which of the following findings would be of GREATEST concern to an IS auditor performing an information security audit of critical server log management activities?

- ☒ Log records can be overwritten before being reviewed.
- ☐ Logging procedures are insufficiently documented.
- ☐ Log records are dynamically into different servers.
- ☐ Logs are monitored using manual processes.

Question 1569

Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

- ☒ Direct access attacks
- ☐ Indirect access attacks
- ☐ Port attack
- ☐ Window attack
- ☐ Social attack
- ☐ None of the choices.

Explanation:

Explanation:

Direct access attacks make use of common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

Question 1570

Which of the following risks could result from inadequate software baselining?

- ☒ Scope creep
- ☐ Sign-off delays
- ☐ Software integrity violations
- ☐ inadequate controls

Explanation:

Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. Choices, C and D may not always result, but choice A is inevitable.

Licensed to Berend Post berend.post@it-university.nl

Question 1571

Which of the following should be the FIRST step when conducting an IT risk assessment?

- ☐ Assess vulnerabilities
- ☒ Identify assets to be protected
- ☐ Evaluate controls in place
- ☐ Identify potential threats

Question 1572

What is an acceptable mechanism for extremely time-sensitive transaction processing?

- ☐ Off-site remote journaling
- ☐ Electronic vaulting
- ☒ Shadow file processing
- ☐ Storage area network

Explanation:

Explanation:

Shadow file processing can be implemented as a recovery mechanism for extremely time- sensitive transaction processing.

Question 1573

Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:

- ☐ pre-BPR process flowcharts.
- ☒ post-BPR process flowcharts.
- ☐ BPR project plans.
- ☐ continuous improvement and monitoring plans.

Explanation:

Explanation:

An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D are incorrect because they are steps within a BPR project.

Licensed to Berend Post berend.post@it-university.nl

Question 1574

A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by the information security manager?

- ☐ Validate that connectivity to the service provider can be made securely.
- ☒ Obtain audit reports on the service providers hosting environment.
- ☐ Review the disaster recovery plans (DRP) of the providers.
- ☐ Align the roles of the organization's and the service providers' staffs.

Question 1575

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- ☐ Palm scan
- ☐ Face recognition
- ☒ Retina scan
- ☐ Hand geometry

Explanation:

Explanation:

Retina scan uses optical technology to map the capillary pattern of an eye's retina. This is highly reliable and has the lowest false-acceptance rate (FAR) among the current biometric methods. Use of palm scanning entails placing a hand on a scanner where a palm's physical characteristics are captured. Hand geometry, one of the oldest techniques, measures the physical characteristics of the user's hands and fingers from a three dimensional perspective. The palm and hand biometric techniques lack uniqueness in the geometry data. In face biometrics, a reader analyzes the images captured for general facial characteristics. Though considered a natural and friendly biometric, the main disadvantage of face recognition is the lack of uniqueness, which means that people looking alike can fool the device.

Question 1576

An organization is replacing a mission-critical system. Which of the following is the BEST implementation strategy to mitigate and reduce the risk of system failure?

- ☐ Stage
- ☐ Phase
- ☒ Parallel
- ☐ Big-bang

Licensed to Berend Post berend.post@it-university.nl

Question 1577

An IS auditor finds that application servers had inconsistent security settings leading to potential vulnerabilities. Which of the following is the BEST recommendation by the IS auditor?

- ☐ Improve the change management process
- ☒ Perform a configuration review
- ☐ Establish security metrics
- ☐ Perform a penetration test

Question 1578

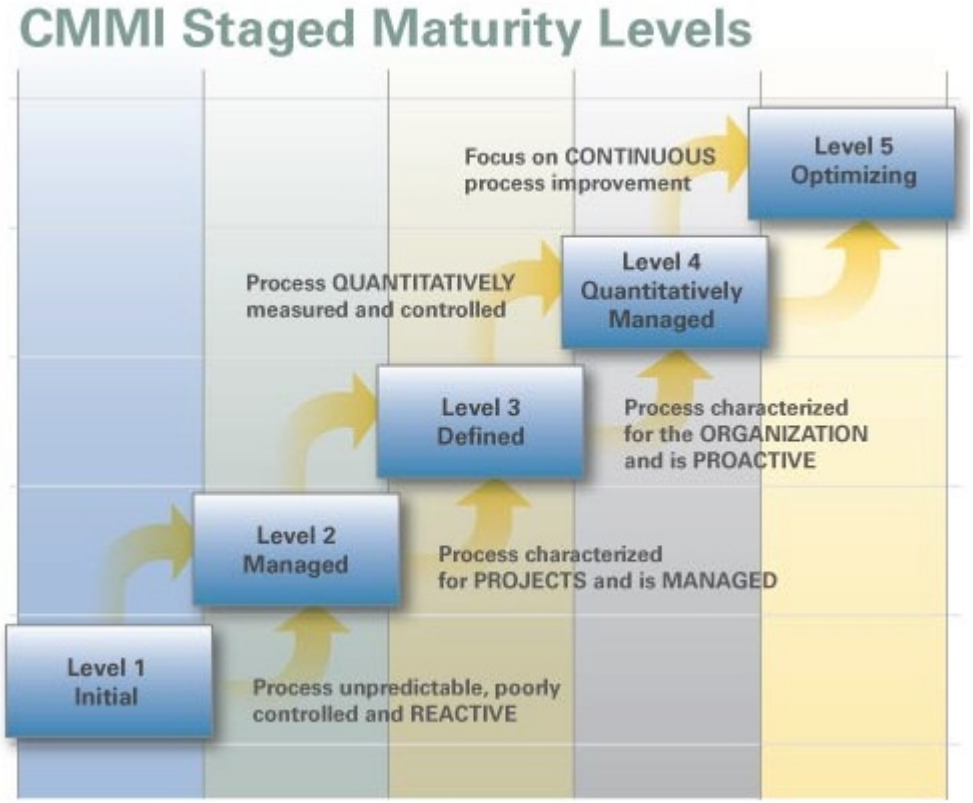
Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

- ☒ Initial, Managed, Defined, Quantitatively managed, optimized
- ☐ Initial, Managed, Defined, optimized, Quantitatively managed
- ☐ Initial, Defined, Managed, Quantitatively managed, optimized
- ☐ Initial, Managed, Quantitatively managed, Defined, optimized

Explanation:

Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.



Licensed to Berend Post berend.post@it-university.nl

A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organizations' software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

Licensed to Berend Post berend.post@it-university.nl

Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.

Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions).

Managed - the process is quantitatively managed in accordance with agreed-upon metrics.

Optimizing - process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Licensed to Berend Post berend.post@it-university.nl

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

The following answers are incorrect:

The other option specified in the option does not provide correct sequence.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

CISSP Official study guide page number 693

Question 1579

An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

- ☒ the probability of error must be objectively quantified.
- ☐ the auditor wishes to avoid sampling risk.
- ☐ generalized audit software is unavailable.
- ☐ the tolerable error rate cannot be determined.

Explanation:

Explanation:

Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples. Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

Licensed to Berend Post berend.post@it-university.nl

Question 1580

Which of the following terms is used more generally for describing concealment routines in a malicious program?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☒ rootkits
- ☐ backdoor
- ☐ None of the choices.

Explanation:

Explanation:

Rootkits can prevent a malicious process from being reported in the process table, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator access. Today, the term is used more generally for concealment routines in a malicious program.

Question 1581

An IS auditor is planning to audit an organization's infrastructure for access, patching, and change management. Which of the following is the BEST way to prioritize the systems?

- ☐ Complexity of the environment
- ☒ Criticality of the system
- ☐ System hierarchy within the infrastructure
- ☐ System retirement plan

Question 1582

An internet-based attack using password sniffing can:

- ☐ enable one party to act as if they are another party.
- ☐ cause modification to the contents of certain transactions.
- ☒ be used to gain access to systems containing proprietary information.
- ☐ result in major problems with billing systems and transaction processing agreements.

Explanation:

Explanation:

Password sniffing attacks can be used to gain access to systems on which proprietary information is stored. Spoofing attacks can be used to enable one party to act as if they are another party. Data modification attacks can be used to modify the contents of certain transactions. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

Licensed to Berend Post berend.post@it-university.nl

Question 1583

Which of the following BEST indicates the effectiveness of an organization's risk management program?

- ☐ Control risk is minimized.
- ☐ Inherent risk is eliminated.
- ☒ Residual risk is minimized.
- ☐ Overall risk is quantified.

Question 1584

An organization has implemented data storage hardware. Which of the following should an IS auditor review to assess if IT is maximizing storage and network utilization?

- ☒ Capacity management plans
- ☐ Downtime statistics
- ☐ The quality management systems
- ☐ Routine and non-routine job schedules

Question 1585

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

- ☐ Pilot
- ☐ Parallel
- ☒ Direct cutover
- ☐ Phased

Explanation:

Explanation:

Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

Question 1586

The BEST test to determine whether an application's internal security controls are configured in compliance with the organization's security standards is an evaluation of the:

- ☐ availability and frequency of security reports
- ☐ intrusion detection system (IDS) logs
- ☐ application's user accounts and passwords
- ☒ business application's security parameter settings

Licensed to Berend Post berend.post@it-university.nl

Question 1587

A TCP/IP-based environment is exposed to the Internet. Which of the following BEST ensures that complete encryption and authentication protocols exist for protecting information while transmitted?

- ☒ Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).
- ☐ A digital signature with RSA has been implemented.
- ☐ Digital certificates with RSA are being used.
- ☐ Work is being completed in TCP services.

Explanation:

Explanation:

Tunnel mode with IP security provides encryption and authentication of the complete IP package. To accomplish this, the AH and ESP services can be nested. Choices B and C provide authentication and integrity. TCP services do not provide encryption and authentication.

Question 1588

Change management procedures are established by IS management to:

- ☒ control the movement of applications from the test environment to the production environment.
- ☐ control the interruption of business operations from lack of attention to unresolved problems.
- ☐ ensure the uninterrupted operation of the business in the event of a disaster.
- ☐ verify that system changes are properly documented.

Explanation:

Explanation:

Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

Question 1589

IS management has decided to replace the current single-server-based local area network (LAN) with three interconnected servers running different operating systems. Existing applications and data on the old server have been exclusively distributed on the new servers. This will MOST likely result in:

- ☐ disclosure of information.
- ☒ multiple authentication.
- ☐ data incompleteness.
- ☐ data unavailability.

Licensed to Berend Post berend.post@it-university.nl

Question 1590

Senior management has approved employees working off-site by using a virtual private network (VPN) connection. It is MOST important for the information security manager to periodically:

- ☐ review firewall configuration
- ☐ review the security policy
- ☐ perform a cost-benefit analysis
- ☒ perform a risk assessment

Question 1591

When auditing an organization's software acquisition process, the BEST way for an IS auditor to understand the software benefits to the organization would be to review the:

- ☐ request for proposal (RFP).
- ☐ feasibility study.
- ☐ alignment with IT strategy.
- ☒ business case.

Question 1592

Controls related to authorized modifications to production programs are BEST tested by:

- ☐ testing only the authorizations to implement the new program.
- ☐ tracing modifications from the executable program back to the original request for change.
- ☐ reviewing only the actual lines of source code changed in the program.
- ☒ tracing modifications from the original request for change forward to the executable program.

Question 1593

An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

- ☒ correlation of semantic characteristics of the data migrated between the two systems.
- ☐ correlation of arithmetic characteristics of the data migrated between the two systems.
- ☐ correlation of functional characteristics of the processes between the two systems.
- ☐ relative efficiency of the processes between the two systems.

Explanation:

Explanation:

Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the

Licensed to Berend Post berend.post@it-university.nl

data is the same in the new as it was in the old system. Arithmetic characteristics represent aspects of data structure and internal definition in the database, and therefore are less important than the semantic characteristics. A review of the correlation of the functional characteristics or a review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

Question 1594

Which of the following is the MOST reliable control to prevent double payments made as a result of payment system batch jobs restarting after processing errors?

- ☐ Database rollback in case of processing errors
- ☐ Review of batch job competition logs
- ☒ Duplicate verification at the last possible point in processing
- ☐ Restart procedures integrated in job controls

Question 1595

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

- ☒ An increased number of people using technology
- ☐ Significant cost savings, through a reduction in the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Explanation:

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:

B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.

D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

Question 1596

A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

- ☐ concurrent access.
- ☐ deadlocks.
- ☐ unauthorized access to data.
- ☒ a loss of data integrity.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

Question 1597

Which of the following would be the FIRST step to help ensure the necessary regulatory requirements are addressed in an organization's cross-border data protection policy?

- ☐ Conduct a risk assessment
- ☒ Perform a gap analysis
- ☐ Conduct stakeholder interviews
- ☐ Perform a business impact analysis

Question 1598

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- ☐ Test data/deck
- ☒ Base-case system evaluation
- ☐ Integrated test facility (ITF)
- ☐ Parallel simulation

Explanation:

Explanation:

A base-case system evaluation uses test data sets developed as part of comprehensive testing programs, it is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

Question 1599

A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

- ☐ Comparing source code
- ☒ Reviewing system log files
- ☐ Comparing object code
- ☐ Reviewing executable and source code integrity

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Source and object code comparisons are ineffective, because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control, because integrity between the executable and source code is automatically maintained.

Question 1600

An organization implemented a mandatory information security awareness training program a year ago. What is the BEST way to determine its effectiveness?

- ☐ Analyze responses from an employee survey on training satisfaction.
- ☐ Analyze results from training completion reports.
- ☒ Analyze results of a social engineering test.
- ☐ Analyze findings from previous audit reports.

Question 1601

An IS auditor reviewing the risk assessment process of an organization should FIRST:

- ☐ identify the reasonable threats to the information assets.
- ☐ analyze the technical and organizational vulnerabilities.
- ☒ identify and rank the information assets.
- ☐ evaluate the effect of a potential security breach.

Explanation:

Explanation:

Identification and ranking of information assets-e.g., data criticality, locations of assets-will set the tone or scope of how to assess risk in relation to the organizational value of the asset. Second, the threats facing each of the organization's assets should be analyzed according to their value to the organization. Third, weaknesses should be identified so that controls can be evaluated to determine if they mitigate the weaknesses. Fourth, analyze how these weaknesses, in absence of given controls, would impact the organization information assets.

Question 1602

A previously agreed-upon recommendation was not implemented because the auditee no longer agrees with the original findings. The IS auditor's FIRST course of action should be to:

- ☐ exclude the finding in the follow-up audit report.
- ☐ escalate the disagreement to the audit committee.
- ☒ assess the reason for the disagreement.
- ☐ require implementation of the original recommendation.

Licensed to Berend Post berend.post@it-university.nl

Question 1603

Internal audit reports should be PRIMARILY written for and communicated to:

- ☒ audit management, as they are responsible for the quality of the audit.
- ☐ external auditors, as they provide an opinion on the financial statements.
- ☐ auditees, as they will eventually have to implement the recommendations.
- ☐ senior management, as they should be informed about the identified risks.

Question 1604

Which of the following is the MOST important reason to use statistical sampling?

- ☐ The results are more defensible
- ☐ It ensures that all relevant cases are covered
- ☒ It reduces time required for testing
- ☐ The results can reduce error rates

Question 1605

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

- ☒ Evidence collected through personal observation
- ☐ Evidence collected through systems logs provided by the organization's security administration
- ☐ Evidence collected through surveys collected from internal staff
- ☐ Evidence collected through transaction reports provided by the organization's IT administration

Explanation:

Explanation:

An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

Question 1606

An organization’s information security department is creating procedures for handling digital evidence that may be used in court. Which of the following would be the MOST important consideration from a risk standpoint?

- ☐ Ensuring the entire security team reviews the evidence
- ☐ Ensuring that analysis is conducted on the original data
- ☐ Ensuring the original data is kept confidential
- ☒ Ensuring the integrity of the data is preserved

Licensed to Berend Post berend.post@it-university.nl

Question 1607

Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?

- ☒ Three users with the ability to capture and verify their own messages
- ☐ Five users with the ability to capture and send their own messages
- ☐ Five users with the ability to verify other users and to send their own messages
- ☐ Three users with the ability to capture and verify the messages of other users and to send their own messages

Explanation:

Explanation:

The ability of one individual to capture and verify messages represents an inadequate segregation, since messages can be taken as correct and as if they had already been verified.

Question 1608

Which of the following is the GREATEST concern with conducting penetration testing on an internally developed application in the production environment?

- ☐ The testing could create application availability issues.
- ☐ The testing may identify only known operating system vulnerabilities.
- ☐ The issues identified during the testing may require significant remediation efforts.
- ☒ Internal security staff may not be qualified to conduct application penetration testing.

Question 1609

During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

- ☒ implement data backup and recovery procedures.
- ☐ Define standards and closely monitor for compliance.
- ☐ Ensure that only authorized personnel can update the database.
- ☐ Establish controls to handle concurrent access problems.

Explanation:

Explanation:

Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, while monitoring for compliance is a detective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

Licensed to Berend Post berend.post@it-university.nl

Question 1610

An IS auditor finds that a mortgage origination team receives customer mortgage applications via a shared repository. Which of the following test procedures is the BEST way to assess whether there are adequate privacy controls over this process?

- ☒ Validate whether the encryption is compliant with the organization's requirements.
- ☐ Validate that data is entered accurately and timely.
- ☐ Validate whether documents are deleted according to data retention procedures.
- ☐ Validate whether complex passwords are required.

Question 1611

The GREATEST benefit of using a prototyping approach in software development is that it helps to:

- ☐ decrease the time allocated for user testing and review
- ☐ minimize scope changes to the system
- ☒ conceptualize and clarify requirements
- ☐ improve efficiency of quality assurance (QA) testing

Question 1612

An organization globally distributes a free phone application that includes a module to gather and report user information. The application includes a privacy notice alerting users to the data gathering. Which of the following presents the GREATEST risk?

- ☐ The data gathering notice is available in only one language.
- ☐ There is no framework to delete personal data.
- ☐ There may be a backlash among users when the data gathering is revealed.
- ☒ The data is not properly encrypted on the application server.

Question 1613

The initial step in establishing an information security program is the:

- ☐ development and implementation of an information security standards manual.
- ☐ performance of a comprehensive security control review by the IS auditor.
- ☒ adoption of a corporate information security policy statement.
- ☐ purchase of security access control software.

Explanation:

Explanation:

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

Licensed to Berend Post berend.post@it-university.nl

Question 1614

The MOST effective method for an IS auditor to determine which controls are functioning in an operating system is to:

- ☒ compare the current configuration to the corporate standard.
- ☐ consult with the systems programmer.
- ☐ consult with the vendor of the system.
- ☐ compare the current configuration to the default configuration.

Question 1615

Which of the following would be MOST useful for determining whether the goals of IT are aligned with the organization's goals?

- ☒ Balanced scorecard
- ☐ Enterprise architecture
- ☐ Key performance indicators
- ☐ Enterprise dashboard

Question 1616

Which of the following procedures would BEST contribute to the reliability of information in a data warehouse?

- ☐ Retaining only current data
- ☐ Storing only a single type of data
- ☒ Maintaining archive data
- ☐ Maintaining current metadata

Question 1617

A maturity model can be used to aid the implementation of IT governance by identifying:

- ☐ critical success factors (CSF)
- ☐ performance drivers
- ☒ improvement opportunities
- ☐ accountabilities

Licensed to Berend Post berend.post@it-university.nl

Question 1618

Which of the following should be used to assess the level of security required to protect information on a corporate network?

- ☐ Data classification
- ☐ Business intelligence
- ☒ Access rights
- ☐ Access control matrix

Question 1619

Iptables is based on which of the following frameworks?

- ☒ Netfilter
- ☐ NetDoom
- ☐ NetCheck
- ☐ NetSecure
- ☐ None of the choices.

Explanation:

Explanation:

ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above.

Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

Question 1620

An IS auditor finds that application servers had inconsistent configurations leading to potential security vulnerabilities. Which of the following should the auditor recommend FIRST?

- ☒ Enforce server baseline standards.
- ☐ Improve change management processes using a workflow tool.
- ☐ Hold the application owner accountable for monitoring metrics.
- ☐ Use a single vendor for the application servers.

Licensed to Berend Post berend.post@it-university.nl

Question 1621

Which of the following controls should be implemented to BEST minimize system downtime for maintenance?

- ☐ Nightly full backups
- ☐ Virtualization
- ☐ Warm site
- ☒ Clustering

Question 1622

An organization's audit charter should:

- ☐ set the enterprise strategic direction.
- ☒ detail the audit objectives.
- ☐ define the auditors' right to access information.
- ☐ include the IS audit plan.

Question 1623

Which of the following would provide the highest degree of server access control?

- ☐ A mantrap-monitored entryway to the server room
- ☐ Host-based intrusion detection combined with CCTV
- ☐ Network-based intrusion detection
- ☒ A fingerprint scanner facilitating biometric access control

Explanation:

Explanation:

A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

Question 1624

An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?

- ☒ Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
- ☐ Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
- ☐ Review the methodology adopted by the organization in choosing the service provider.
- ☐ Review the accreditation of the third-party service provider's staff.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Reviewing whether the service provider's business continuity plan (BCP) process is aligned with the organization's BCP and contractual obligations is the correct answer since an adverse effect or disruption to the business of the service provider has a direct bearing on the organization and its customers. Reviewing whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster is not the correct answer since the presence of penalty clauses, although an essential element of a SLA, is not a primary concern.

Choices C and D are possible concerns, but of lesser importance.

Question 1625

During the review of a business process reengineering project, the PRIMARY concern of an IS auditor is to determine whether the new business model:

- ☐ is aligned with industry best practices.
- ☒ is aligned with organizational goals.
- ☐ leverages benchmarking results.
- ☐ meets its key performance measures.

Question 1626

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

- ☒ The preservation of the chain of custody for electronic evidence
- ☐ Time and cost savings
- ☐ Efficiency and effectiveness
- ☐ Ability to search for violations of intellectual property rights

Explanation:

Explanation:

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

Licensed to Berend Post berend.post@it-university.nl

Question 1627

What should be the GREATEST concern to an IS auditor when employees use portable media (MP3 players, flash drives)?

- ☒ The copying of sensitive data on them
- ☐ The copying of songs and videos on them
- ☐ The cost of these devices multiplied by all the employees could be high
- ☐ They facilitate the spread of malicious code through the corporate network

Explanation:

Explanation:

The MAIN concern with MP3 players and flash drives is data leakage, especially sensitive information. This could occur if the devices were lost or stolen. The risk when copying songs and videos is copyright infringement, but this is normally a less important risk than information leakage. Choice C is hardly an issue because employees normally buy the portable media with their own funds. Choice D is a possible risk, but not as important as information leakage and can be reduced by other controls.

Question 1628

A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server. Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

- ☒ A continual server replication process
- ☐ A property tested offline backup system
- ☐ A property configured firewall
- ☐ Employee training on ransomware

Question 1629

Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

- ☒ Developments may result in hardware and software incompatibility.
- ☐ Resources may not be available when needed.
- ☐ The recovery plan cannot be tested.
- ☐ The security infrastructures in each company may be different.

Explanation:

Explanation:

If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based

Licensed to Berend Post berend.post@it-university.nl

walkthroughs, and possibly by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

Question 1630

In a high-volume, real-time system, the MOST effective technique by which to continuously monitor and analyze transaction processing is:

- ☐ integrated test facility (ITF).
- ☐ embedded audit modules.
- ☐ parallel simulation.
- ☒ transaction tagging.

Question 1631

Who is responsible for ensuring that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures?

- ☐ Project Sponsor
- ☒ Security Officer
- ☐ User Management
- ☐ Senior Management

Explanation:

Security Officer ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

For the CISA exam you should know the information below about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management -Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?

Licensed to Berend Post berend.post@it-university.nl

How reliable is the software?

How effective is the software?

Is the software easy to use?

How easy is to transfer or adapt old data from preexisting software to this environment?

Is it possible to add new functions?

Does it meet regulatory requirement?

Project Steering Committee -Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

System Development Management -Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager -Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor - Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team -Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team -Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Licensed to Berend Post berend.post@it-university.nl

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Project Sponsor - Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

User Management -Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management - Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 150

Question 1632

Which of the following type of testing uses a set of test cases that focus on control structure of the procedural design?

- ☐ Interface testing
- ☒ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Unit testing is the testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

For CISA exam you should know below types of testing:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the system's ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Licensed to Berend Post berend.post@it-university.nl

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.

QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include:

Definition of test strategies and procedure.

Design of test cases and scenarios

Execution of the tests.

Utilization of the result to verify system readiness.

Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team.

Final Acceptance Testing – During this testing phase the defined methods of testing to apply should be incorporated into the organization's QA methodology.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 166

Question 1633

Functional acknowledgements are used:

- ☒ as an audit trail for EDI transactions.
- ☐ to functionally describe the IS department.
- ☐ to document user roles and responsibilities.
- ☐ as a functional description of application software.

Explanation:

Explanation:

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

Question 1634

Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?

- ☐ Virtual tape libraries
- ☐ Disk-based snapshots
- ☒ Continuous data backup
- ☐ Disk-to-tape backup

Explanation:

Explanation:

The recovery point objective (RPO) is based on the acceptable data loss in the case of a disruption. In this scenario the organization needs a short RPO. Virtual tape libraries, disk- based snapshots and disk-to-tape backup would require time to complete the backup, while continuous data backup happens online (in real time).

Licensed to Berend Post berend.post@it-university.nl

Question 1635

A hub is a device that connects:

- ☐ two LANs using different protocols.
- ☐ a LAN with a WAN.
- ☐ a LAN with a metropolitan area network (MAN).
- ☒ two segments of a single LAN.

Explanation:

Explanation:

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device.

Question 1636

As IS auditor discovers that due to resource constraints, a database administrator (DBA) is responsible for developing and executing changes into the production environment. Which of the following should the auditor do FIRST?

- ☐ Identify whether any compensating controls exist
- ☐ Report a potential segregation of duties (SoD) violation
- ☐ Determine whether another database administrator could make the changes
- ☒ Ensure a change management process is followed prior to implementation

Question 1637

Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following?

- ☐ Unsynchronized transactions
- ☒ Unauthorized transactions
- ☐ Inaccurate transactions
- ☐ Incomplete transactions

Explanation:

Explanation:

Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

Licensed to Berend Post berend.post@it-university.nl

Question 1638

The GREATEST risk of database denormalization is:

- ☒ decreased performance.
- ☐ loss of data confidentiality.
- ☐ loss of database integrity.
- ☐ incorrect metadata.

Question 1639

The IS auditor has identified a potential fraud perpetrated by the network administrator. The IS auditor should:

- ☐ issue a report to ensure a timely resolution
- ☒ review the audit finding with the audit committee prior to any other discussions
- ☐ perform more detailed tests prior to disclosing the audit results
- ☐ share the potential audit finding with the security administrator

Question 1640

Which of the following provides the best evidence of the adequacy of a security awareness program?

- ☐ The number of stakeholders including employees trained at various levels
- ☐ Coverage of training at all locations across the enterprise
- ☐ The implementation of security devices from different vendors
- ☒ Periodic reviews and comparison with best practices

Explanation:

Explanation:

The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

Question 1641

In which of the following database models is the data represented in terms of tulles and grouped into relations?

- ☐ Hierarchical database model
- ☐ Network database model
- ☒ Relational database model
- ☐ Object-relational database model

Explanation:

In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

Hierarchical database model

Network model

Relational model

Object-relational database models

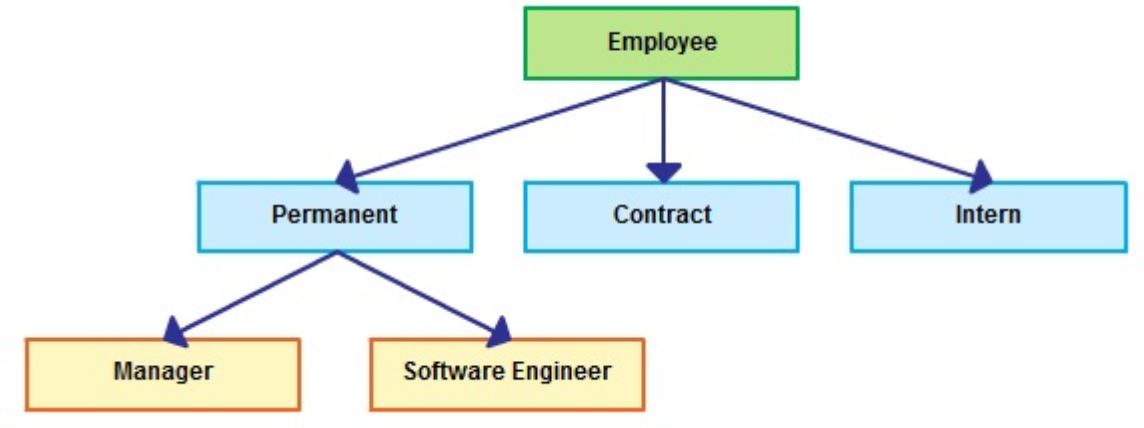
Hierarchical database model

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Hierarchical database model

Licensed to Berend Post berend.post@it-university.nl



Network database model

The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

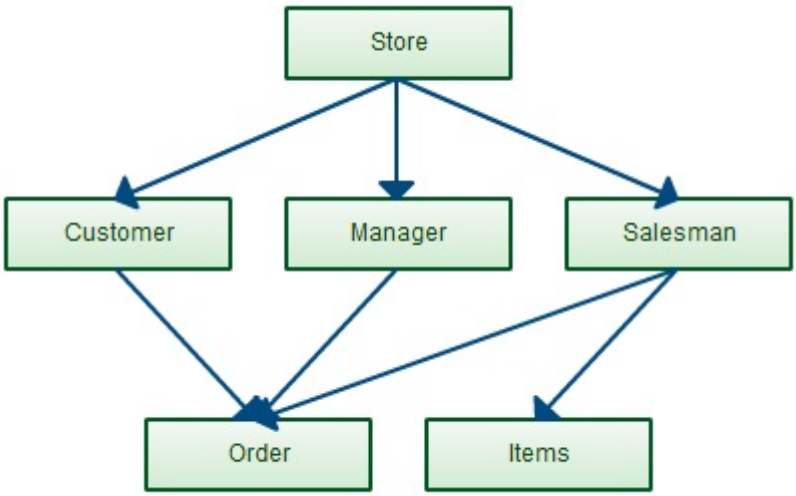
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.

Network Database model

Licensed to Berend Post berend.post@it-university.nl



Relational database model

In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

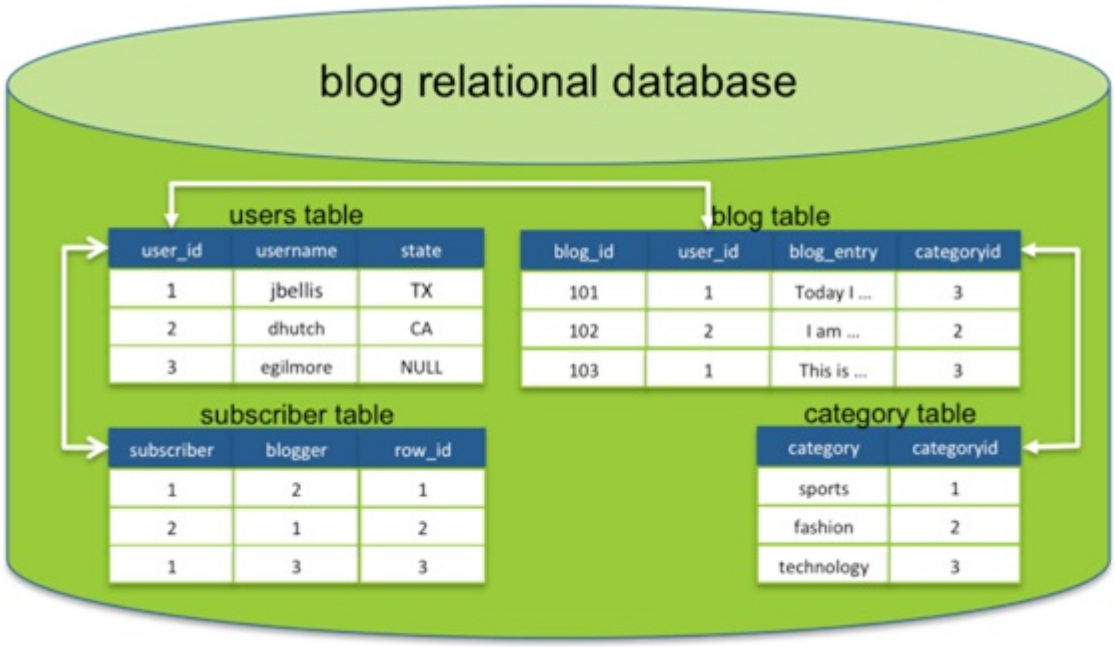
In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.

Relational database model

Licensed to Berend Post berend.post@it-university.nl



Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an

Licensed to Berend Post berend.post@it-university.nl

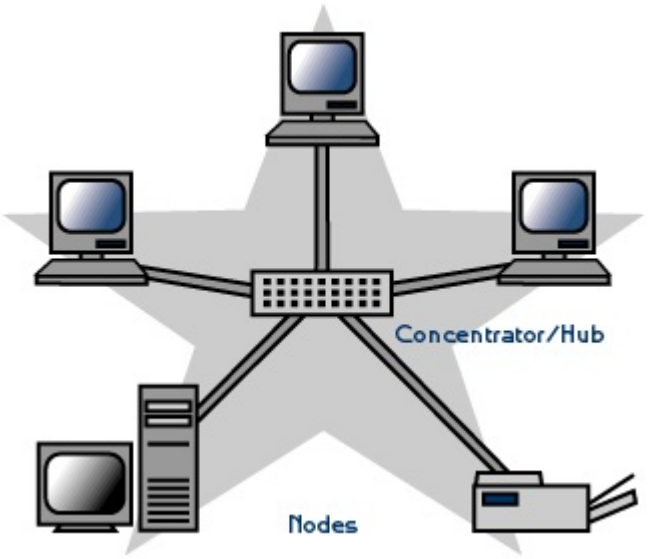
object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 254

Question 1642

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☒ Star
- ☐ Ring
- ☐ Mesh

Explanation:

For your exam you should know the information below related to LAN topologies:

LAN Topologies

Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device

Licensed to Berend Post berend.post@it-university.nl

location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

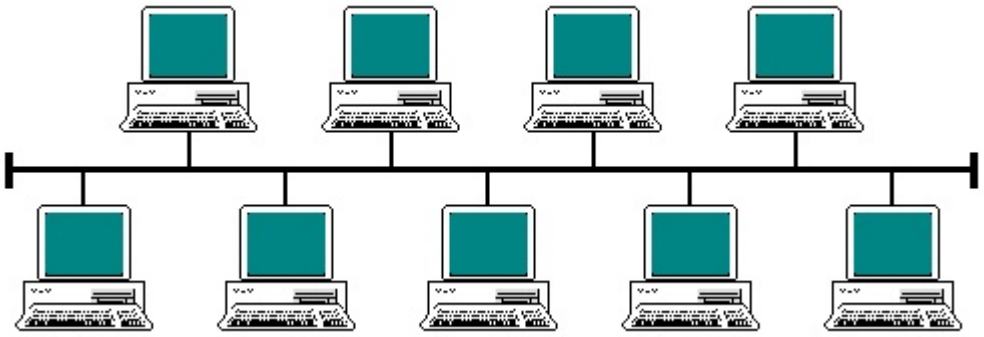
Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology

Graphic from:



Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly

Licensed to Berend Post berend.post@it-university.nl

the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

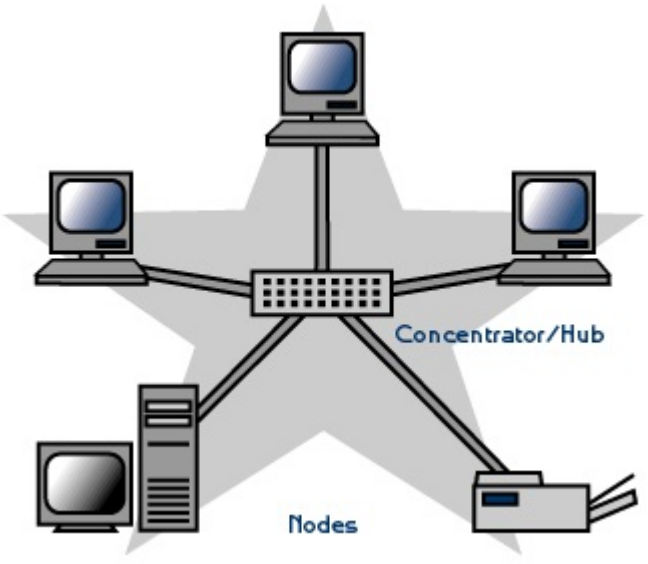
In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure.

Star Topology



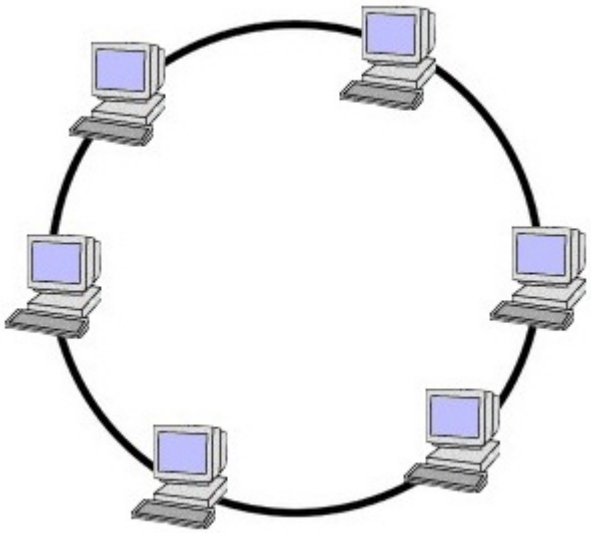
Ring

A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

Licensed to Berend Post berend.post@it-university.nl

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology



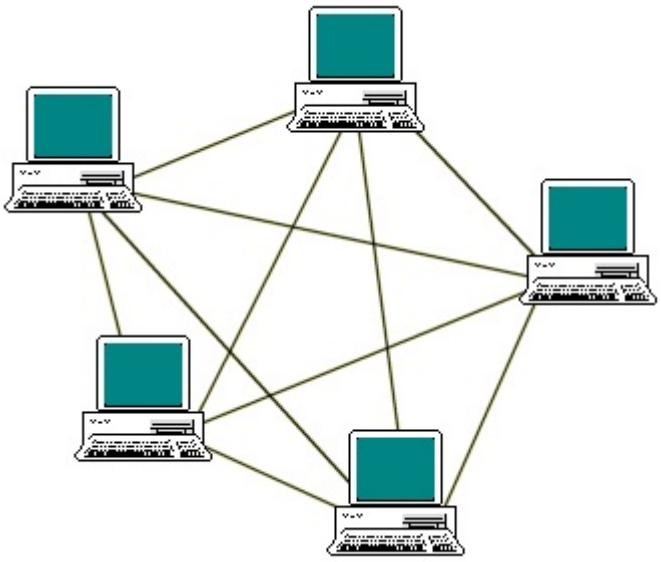
Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.

Mesh Topology

Licensed to Berend Post berend.post@it-university.nl



Fully connected mesh topology

A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:

The other options presented are not valid.

The following reference(s) were/was used to create this question:

CISA review manual 2014, Page number 262

Licensed to Berend Post berend.post@it-university.nl

Question 1643

Identify the payment model from description presented below:
A users write an electronic check, which is digitally signed with instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

- ☐ Electronic Money Model
- ☒ Electronics Checks model
- ☐ Electronic transfer model
- ☐ Electronic withdraw model

Explanation:

Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems – the issuer and the user. An issuer is an entity that operates the payment service. An issuer holds the items that the payment represents. The user of the payment service performs two main functions- making payments and receiving payments – and therefore can be described as a payer or payee receptively.

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Check Model -Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then

Licensed to Berend Post berend.post@it-university.nl

verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

The following were incorrect answers:

Electronic Money Model -The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

Electronic Transfer Model -Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

Electronic Withdraw Model – Not a valid type of payment system.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 183

Question 1644

An organization is deciding whether to outsource its customer relationship management systems to a provider located in another country. Which of the following should be the PRIMARY influence in the outsourcing decision?

- ☐ Time zone differences
- ☐ The service provider's disaster recovery plan
- ☒ Cross-border privacy laws
- ☐ Current geopolitical conditions

Licensed to Berend Post berend.post@it-university.nl

Question 1645

When should systems administrators first assess the impact of applications or systems patches?

- ☐ Within five business days following installation
- ☒ Prior to installation
- ☐ No sooner than five business days following installation
- ☐ Immediately following installation

Explanation:

Explanation:

Systems administrators should always assess the impact of patches before installation.

Question 1646

A design company has multiple name and address files for its customers in several of its independent systems. Which of the following is the BEST control to ensure that the customer name and address agree across all files?

- ☒ Use of hash totals on customer records
- ☐ Periodic review of each master file by management
- ☐ Matching of records and review of exception reports
- ☐ Use of authorized master file change forms

Question 1647

An IS steering committee should:

- ☐ include a mix of members from different departments and staff levels.
- ☐ ensure that IS security policies and procedures have been executed properly.
- ☒ have formal terms of reference and maintain minutes of its meetings.
- ☐ be briefed about new trends and products at each meeting by a vendor.

Explanation:

Explanation:

It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

Licensed to Berend Post berend.post@it-university.nl

Question 1648

Which of the following will BEST protect an organization against spear phishing?

- ☐ Email content filtering
- ☐ Acceptable use policy
- ☒ End-user training
- ☐ Antivirus software

Question 1649

Which type of control is being implemented when a biometric access device is installed at the entrance to a facility?

- ☒ Preventive
- ☐ Deterrent
- ☐ Corrective
- ☐ Detective

Question 1650

An IS auditor is assessing risk associated with peer-to-peer file sharing within an organization. Which of the following should be of GREATEST concern?

- ☐ File-sharing policies have not been reviewed since last year
- ☐ Only some employees are required to attend security awareness training
- ☒ Not all devices are running antivirus programs
- ☐ The organization does not have an efficient patch management process

Question 1651

Who is responsible for providing adequate physical and logical security for IS program, data and equipment?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☒ Security Administrator

Explanation:

Security administrator are responsible for providing adequate physical and logical security for IS programs, data and equipment.

For CISA exam you should know below roles in an organization

Licensed to Berend Post berend.post@it-university.nl

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Data Owner- These peoples are generally managers and directors responsible for using information for running and controlling the business.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 361

Question 1652

When developing a risk management program, what is the FIRST activity to be performed?

- ☐ Threat assessment
- ☐ Classification of data
- ☒ Inventory of assets
- ☐ Criticality analysis

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

Question 1653

Which of the following ISO/OSI layers performs transformations on data to provide a standardized application interface and to provide common communication services such as encryption?

- ☐ Application layer
- ☐ Session layer
- ☒ Presentation layer
- ☐ Transport layer

Explanation:

The presentation layer (ISO/OSI layer 6) performs transformations on data to provide a standardized application interface and to provide common communication services such as encryption, text compression and reformatting. The function of the presentation layer is to ensure that the format of the data submitted by the application layer conforms to the applicable network standard.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 119).

Question 1654

Who is responsible for implementing cost-effective controls in an automated system?

- ☐ Security policy administrators
- ☒ Business unit management
- ☐ Senior management
- ☐ Board of directors

Explanation:

Explanation:

Business unit management is responsible for implementing cost-effective controls in an automated system.

Licensed to Berend Post berend.post@it-university.nl

Question 1655

Which of the following is the PRIMARY risk when business units procure IT assets without IT involvement?

- ☒ Corporate procurement standards are not followed.
- ☐ The business units want IT to be responsible for maintenance costs.
- ☐ Data security requirements are not considered.
- ☐ System inventory becomes inaccurate.

Question 1656

Network Data Management Protocol (NDMP) technology should be used for backup if:

- ☒ a network attached storage (NAS) appliance is required.
- ☐ the use of TCP/I P must be avoided.
- ☐ file permissions that can not be handled by legacy backup systems must be backed up.
- ☐ backup consistency over several related data volumes must be ensured.

Explanation:

Explanation:NDMP defines three kinds of services: a data service that interfaces with the primary storage to be backed up or restored, a tape service that interfaces with the secondary storage (primarily a tape device), and a translator service performing translations including multiplexing multiple data streams into one data stream and vice versa. NDMP services interact with each other. The result of this interaction is the establishment of an NDMP control session if the session is being used to achieve control for the backup or restore operation. It would result in an NDMP data session if the session is being used to transfer actual file system or volume data (including metadata). Control sessions are always TCP/IP-based, but data streams can be TCP/IP-or SAN-based. NDMP is more or less NAS-centric and defines a way to back up and restore data from a device, such as a NAS appliance, on which it is difficult to install a backup software agent, in the absence of NDMP, this data must be backed up as a shared drive on the LAN, which is accessed via network file protocols, such as Common Internet File System (CIFS) or Network File System (NFS), degrading backup performance. NDMP works on a block level for transferring payload data (file content) but metadata and traditional file system information needs to be handled by legacy backup systems that initiate NDMP data movement. NDMP does not know about nor takes care of consistency issues regarding related volumes (e.g., a volume to store database files, a volume to store application server data and a volume to store web server data). NDMP can be used to do backups in such an environment (e.g., SAP) but the logic required either must be put into a dedicated piece of software or must be scripted into the legacy backup software.

Licensed to Berend Post berend.post@it-university.nl

Question 1657

An IT steering committee should review information systems PRIMARILY to assess:

- ☒ whether IT processes support business requirements.
- ☐ if proposed system functionality is adequate
- ☐ the stability of existing software.
- ☐ the complexity of installed technology.

Explanation:

Explanation:

The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

Question 1658

Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

- ☐ Field checks
- ☐ Control totals
- ☐ Reasonableness checks
- ☒ A before-and-after maintenance report

Explanation:

Explanation:

A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

Question 1659

Which of the following would be a result of utilizing a top-down maturity model process?

- ☐ A means of benchmarking the effectiveness of similar processes with peers
- ☐ Identification of older, more established processes to ensure timely review
- ☒ Identification of processes with the most improvement opportunities
- ☐ A means of comparing the effectiveness of other processes within the enterprise

Licensed to Berend Post berend.post@it-university.nl

Question 1660

Which of the following is the PRIMARY responsibility of an organization's information security function?

- ☐ Reviewing unauthorized attempts to access sensitive files
- ☒ Managing the organization's security procedures
- ☐ Approving access to data files
- ☐ Installing network security programs

Question 1661

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- ☐ Install the vendor's security fix for the vulnerability.
- ☐ Block the protocol traffic in the perimeter firewall.
- ☐ Block the protocol traffic between internal network segments.
- ☒ Stop the service until an appropriate security fix is installed.

Explanation:

Explanation:

Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

Question 1662

Which of the following type of lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor/reader to gain access?

- ☐ Bolting door locks
- ☐ Combination door lock
- ☒ Electronic door lock
- ☐ Biometric door lock

Explanation:

Electronic door lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

For CISA exam you should know below types of lock

Licensed to Berend Post berend.post@it-university.nl

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

The Combination door lock or cipher lock uses a numeric key pad or dial to gain entry, and is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

The following were incorrect answers:

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

The Combination door lock or cipher lock uses a numeric key pad or dial to gain entry, and is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 376

Licensed to Berend Post berend.post@it-university.nl

Question 1663

Which of the following would be MOST critical for an IS auditor to look for when evaluating fire precautions in a manned data center located in the upper floor of a multi-story building?

- ☐ Existence of handheld fire extinguishers in highly visible locations
- ☐ Documentation of regular inspections by the local fire department
- ☐ Adequacy of the HVAC system throughout the facility
- ☒ Documentation of tested emergency evacuation plans

Question 1664

Which of the following layer of an enterprise data flow architecture is responsible for data copying, transformation in Data Warehouse (DW) format and quality control?

- ☒ Data Staging and quality layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Explanation:

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Licensed to Berend Post berend.post@it-university.nl

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Licensed to Berend Post berend.post@it-university.nl

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and

Licensed to Berend Post berend.post@it-university.nl

analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 1665

When should application controls be considered within the system-development process?

- ☐ After application unit testing
- ☐ After application module testing
- ☐ After applications systems testing
- ☒ As early as possible, even in the development of the project's functional specifications

Explanation:

Explanation:

Application controls should be considered as early as possible in the system- development process, even in the development of the project's functional specifications.

Question 1666

The quality assurance (QA) function should be prevented from:

- ☐ developing naming conventions.
- ☐ establishing analysis techniques.
- ☒ amending review procedures.
- ☐ changing programs for business functions.

Licensed to Berend Post berend.post@it-university.nl

Question 1667

Which of the following BEST determines if a batch update job was completed?

- ☐ Reviewing the job log
- ☒ Testing a sample of transactions
- ☐ Reviewing a copy of the script
- ☐ Obtaining process owner confirmation

Question 1668

What is an IS auditor's BEST recommendation for management if a network vulnerability assessment confirms that critical patches have not been applied since the last assessment?

- ☒ Implement a process to test and apply appropriate patches.
- ☐ Apply available patches and continue periodic monitoring.
- ☐ Configure servers to automatically apply available patches.
- ☐ Remove unpatched devices from the network.

Question 1669

Which of the following is the BEST type of backup to minimize the associated time and media?

- ☒ Differential
- ☐ Incremental
- ☐ Mirror
- ☐ Compressed full

Question 1670

An offsite information processing facility:

- ☒ should have the same amount of physical access restrictions as the primary processing site.
- ☐ should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
- ☐ should be located in proximity to the originating site, so it can quickly be made operational.
- ☐ need not have the same level of environmental monitoring as the originating site.

Explanation:

Explanation:

An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site. The offsite facility should possess the same level of environmental monitoring and control as the originating site.

Licensed to Berend Post berend.post@it-university.nl

Question 1671

Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor's BEST course of action would be to determine if:

- ☐ the domain controller was classified for high availability.
- ☐ the network traffic was being monitored.
- ☐ the patches were updated.
- ☒ the logs were monitored.

Question 1672

An IS auditor is evaluating the security of an organization's data backup process, which includes the transmission of daily incremental backups to a dedicated offsite server. Which of the following findings poses the GREATEST risk to the organization?

- ☒ Backup transmissions are not encrypted
- ☐ Backup transmissions occasionally fail
- ☐ Data recovery testing is conducted once per year
- ☐ The archived data log is incomplete

Question 1673

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

- ☒ Availability of online network documentation
- ☐ Support of terminal access to remote hosts
- ☐ Handling file transfer between hosts and interuser communications
- ☐ Performance management, audit and control

Explanation:

Explanation:

Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands. Choices B, C and D are examples of network operating systems functions.

Licensed to Berend Post berend.post@it-university.nl

Question 1674

The directory system of a database-management system describes:

- ☐ The access method to the data
- ☒ The location of data AND the access method
- ☐ The location of data
- ☐ Neither the location of data NOR the access method

Explanation:

Explanation:

The directory system of a database-management system describes the location of data and the access method.

Question 1675

Phishing attack works primarily through:

- ☒ email and hyperlinks
- ☐ SMS
- ☐ chat
- ☐ email attachment
- ☐ news
- ☐ file download
- ☐ None of the choices.

Explanation:

Explanation:

"Phishing applies to email appearing to come from a legitimate business, requesting "verification"" of information and warning of some dire consequence if it is not done. The letter usually contains a link to a fradulent web page that looks legitimate and has a form requesting everything from a home address to an ATM card's PIN."

Question 1676

Which of the following is the BEST preventative control to protect the confidentiality of data on a corporate smartphone in the event it is lost?

- ☐ Encryption of the data stored on the device
- ☐ Biometric authentication for the device
- ☐ Password for device authentication
- ☒ Remote data wipe program

Licensed to Berend Post berend.post@it-university.nl

Question 1677

Which of the following layer of an OSI model ensures that messages are delivered error-free, in sequence, and with no losses or duplications?

- ☐ Application layer
- ☐ Presentation layer
- ☐ Session layer
- ☒ Transport layer

Explanation:

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

For your exam you should know below information about OSI model:

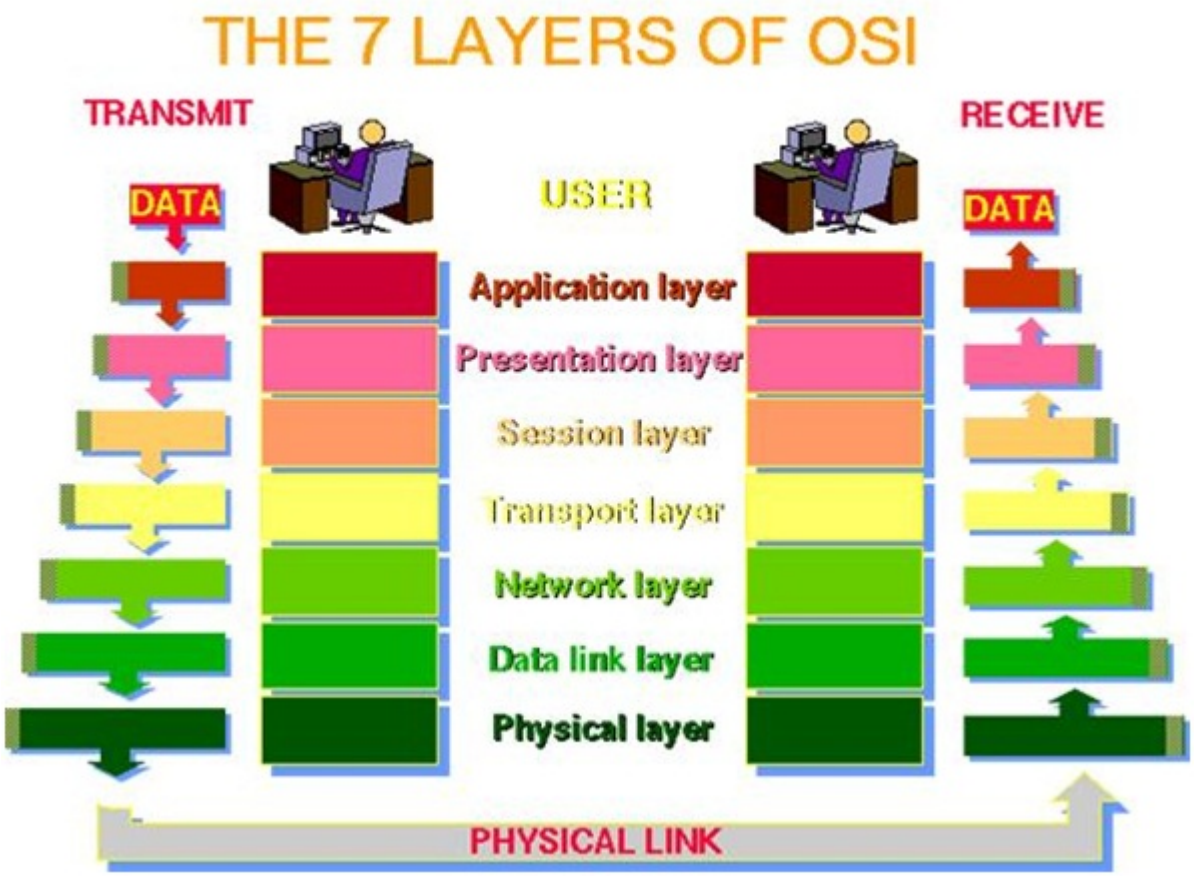
The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower

Licensed to Berend Post berend.post@it-university.nl

layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

Licensed to Berend Post berend.post@it-university.nl

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

Licensed to Berend Post berend.post@it-university.nl

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software

Licensed to Berend Post berend.post@it-university.nl

(and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Application Layer - The application layer serves as the window for users and application processes to access network services.

Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Session layer - The session layer allows session establishment between processes running on different stations.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Question 1678

The objective of concurrency control in a database system is to:

- ☐ restrict updating of the database to authorized users.
- ☒ prevent integrity problems when two processes attempt to update the same data at the same time.
- ☐ prevent inadvertent or unauthorized disclosure of data in the database.
- ☐ ensure the accuracy, completeness and consistency of data.

Explanation:

Explanation:

Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users, and controls such as passwords prevent the inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

Licensed to Berend Post berend.post@it-university.nl

Question 1679

Which policy helps an auditor to gain a better understanding of biometrics system in an organization?

- ☒ BIMS Policy
- ☐ BOMS Policy
- ☐ BMS Policy
- ☐ BOS Policy

Explanation:

The auditor should use a Biometric Information Management System (BIMS) Policy to gain better understanding of the biometric system in use.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution and processing of biometrics data encompassing:

Data integrity, authenticity and non-repudiation

Management of biometric data across its life cycle – compromised of the enrollment, transmission and storage, verification, identification, and termination process

Usage of biometric technology, including one-to-one and one-to-many matching, for identification and authentication

Application of biometric technology for internal and external, as well as logical and physical access control

Encapsulation of biometric data

Security of the physical hardware used throughout the biometric data life cycle

Techniques for integrity and privacy protection of biometric data.

Management should develop and approve a Biometric Information Management and Security (BIMS) policy. The auditor should use the BIMS policy to gain better understanding of the biometric system in use. With respect to testing, the auditor should make sure this policy has been developed and biometric information system is being secured appropriately.

The identification and authentication procedures for individual enrollment and template creation should be specified in BIMS policy.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

All other choices presented were incorrect answers because they are not valid policies.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 331 and 332

Question 1680

Who is mainly responsible for protecting information assets they have been entrusted with on a daily basis by defining who can access the data, it's sensitivity level, type of access, and adhering to corporate information security policies?

- ☒ Data Owner
- ☐ Security Officer
- ☐ Senior Management
- ☐ End User

Explanation:

The Data Owner is the person who has been entrusted with a data set that belong to the company. As such they are responsible to classify the data according to it's value and sensitivity. The Data Owner decides who will get access to the data, what type of access would be granted. The Data Owner will tell the Data Custodian or System Administrator what access to configure within the systems.

A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.

The following answers are incorrect:

Executive Management/Senior Management - Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know.

Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals,

Licensed to Berend Post berend.post@it-university.nl

such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines.

End User - The end user does not decide on classification of the data

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 108

Official ISC2 guide to CISSP CBK 3rd Edition Page number 342

Question 1681

The PRIMARY purpose of asset valuation for the management of information security is to:

- ☐ eliminate the least significant assets.
- ☐ provide a basis for asset classification.
- ☒ determine the value of each asset.
- ☐ prioritize risk management activities.

Question 1682

Which of the following is an effective method for controlling downloading of files via FTP?

- ☐ An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
- ☒ An application-layer gateway, or proxy firewall
- ☐ A circuit-level gateway
- ☐ A first-generation packet-filtering firewall

Explanation:

Explanation:

Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

Licensed to Berend Post berend.post@it-university.nl

Question 1683

During an audit of information security procedures of a large retailer's online store, an IS auditor notes that operating system (OS) patches are automatically deployed upon release. Which of the following should be of GREATEST concern to the auditor?

- ☐ Patches are in conflict with current licensing agreements.
- ☐ Patches are pushed from the vendor increasing Internet traffic.
- ☐ Patches are not reflected in the configuration management database.
- ☒ Patches are not tested before installation on critical servers.

Question 1684

Identify the correct sequence which needs to be followed as a chain of event in regards to evidence handling in computer forensics?

- ☐ Identify, Analyze, preserve and Present
- ☐ Analyze, Identify, preserve and present
- ☐ Preserve, Identify, Analyze and Present
- ☒ Identify, Preserve, Analyze and Present

Explanation:

There are 4 major considerations in the chain of event in regards to evidence in computer forensics:

Identify -Refers to identification of information that is available and might form evidence of an accident

Preserve -Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court law.

Analyze – Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format. Interpreting the data requires an in-depth knowledge of how different pieces of evidences may fit together. The analysis should be performed using an image of media and not the original.

Present -Involves a presentation of the various audiences such as management, attorneys, court, etc.Acceptance of evidence depends upon the manner of presentation, qualification of the presenter, and credibility of the process used to preserve and analyze the evidence.

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

The other options presented are not a valid sequence which needs to be followed in the chain of events in regards to evidence in computer forensic.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number367

Question 1685

When developing an incident response plan, the information manager should:

- ☐ allow IT to decide which systems can be removed from the infrastructure
- ☒ include response scenarios that have been approved previously by business management
- ☐ require IT to invoke the business continuity plan
- ☐ determine recovery time objectives (RTOs)

Question 1686

Which of the following control fixes a component or system after an incident has occurred?

- ☐ Deterrent
- ☐ Preventive
- ☒ Corrective
- ☐ Recovery

Explanation:

Explanation:

Corrective control fixes components or systems after an incident has occurred

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite.

Licensed to Berend Post berend.post@it-university.nl

Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Licensed to Berend Post berend.post@it-university.nl

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Licensed to Berend Post berend.post@it-university.nl

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring

Recovery - Recovery controls are intended to bring the environment back to regular operations

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 1687

Which of the following is MOST appropriate to prevent unauthorized retrieval of confidential information stored in a business application system?

- ☐ Apply single sign-on for access control.
- ☒ Enforce an internal data access policy.
- ☐ Enforce the use of digital signatures.
- ☐ Implement segregation of duties.

Licensed to Berend Post berend.post@it-university.nl

Question 1688

Which of the following cloud computing service model is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components?

- ☐ Software as a service
- ☐ Data as a service
- ☐ Platform as a service
- ☒ Infrastructure as a service

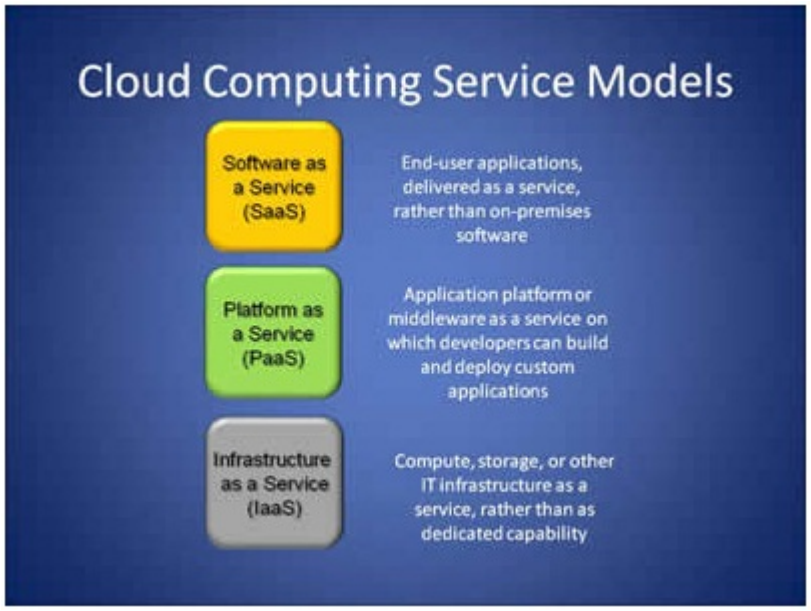
Explanation:

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

For your exam you should know below information about Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing



Cloud computing service models:

Cloud computing service models

Licensed to Berend Post berend.post@it-university.nl

Software as a Service (Seas)

Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for Seas. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for Seas distribution.

Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for Seas distribution and use.

Benefits of the Seas model include:

easier administration

automatic updates and patch management

compatibility: All users will have the same version of software.

easier collaboration, for the same reason

global accessibility.

Platform as a Service (Peas)

Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Where Iasi is the “raw IT network,” Peas is the software environment that runs on top of the IT network.

Platform as a Service (Peas) is an outgrowth of Software as a Service (Seas), a software distribution model in which hosted software applications are made available to customers over the Internet. Peas has several advantages for developers. With Peas, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international

Licensed to Berend Post berend.post@it-university.nl

boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

On the downside, Peas involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

Infrastructure as a Service (Iasi)

Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Characteristics and components of Iasi include:

Utility computing service and billing model.

Automation of administrative tasks.

Dynamic scaling.

Desktop virtualization.

Policy-based services.

Internet connectivity.

Infrastructure as a Service is sometimes referred to as Hardware as a Service (HaaS).

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.

 Licensed to Berend Post berend.post@it-university.nl

Software as a service - Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. Seas is closely related to the ASP (application service provider) and on demand computing software delivery models.

Platform as a service - Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689

http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

Question 1689

An organization is concerned about duplicate vendor payments on a complex system with a high volume of transactions. Which of the following would be MOST helpful to an IS auditor to determine whether duplicate vendor payments exist?

- ☒ Computer-assisted technique
- ☐ Stop-and-go testing
- ☐ Statistical sampling
- ☐ Judgmental sampling

Question 1690

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- ☐ Paper test
- ☐ Post test
- ☒ Preparedness test
- ☐ Walk-through

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. A paper test is a walkthrough of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution. A paper test usually precedes the preparedness test. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third- party systems. A walkthrough is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

Question 1691

During an audit, the client learns that the IS auditor has recently completed a similar security review at a competitor. The client inquires about the competitor's audit results. What is the BEST way for the auditor to address this inquiry?

- ☒ Explain that it would be inappropriate to discuss the results of another audit client.
- ☐ Escalate the question to the audit manager for further action.
- ☐ Discuss the results of the audit omitting specifics related to names and products.
- ☐ Obtain permission from the competitor to use the audit results as examples for future clients.

Question 1692

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- ☒ sufficient evidence will be collected.
- ☐ all significant deficiencies identified will be corrected within a reasonable period.
- ☐ all material weaknesses will be identified.
- ☐ audit costs will be kept at a minimum level.

Explanation:

Explanation:

Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

Licensed to Berend Post berend.post@it-university.nl

Question 1693

Which of the following types of attack makes use of unfiltered user input as the format string parameter in the print () function of the C language?

- ☐ buffer overflows
- ☒ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Explanation:

Explanation:

Format string attacks are a new class of vulnerabilities recently discovered. It can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as print (). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token.

Question 1694

Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

- ☐ A disaster recovery plan
- ☐ Customer references for the alternate site provider
- ☐ Processes for maintaining the disaster recovery plan
- ☒ Results of tests and drills

Explanation:

Explanation:

Plans are important, but mere plans do not provide reasonable assurance unless tested. References for the alternate site provider and the existence and maintenance of a disaster recovery plan are important, but only tests and drills demonstrate the adequacy of the plans and provide reasonable assurance of an organization's disaster recovery readiness.

Question 1695

During a post-incident review. the sequence and correlation of actions must be analyzed PRIMARLY based on:

- ☐ interviews with personnel
- ☐ a consolidated event time line
- ☒ logs from systems involved
- ☐ documents created during the incident

Licensed to Berend Post berend.post@it-university.nl

Question 1696

The MOST significant security concerns when using flash memory (e.g., USB removable disk) is that the:

- ☐ contents are highly volatile.
- ☐ data cannot be backed up.
- ☒ data can be copied.
- ☐ device may not be compatible with other peripherals.

Explanation:

Explanation: Unless properly controlled, flash memory provides an avenue for anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

Question 1697

Which of the following is the MOST important part of an incident response plan?

- ☐ Recovery point objective (RPO)
- ☒ Recovery time objective (RTO)
- ☐ Mean time to report (MTR)
- ☐ Business impact analysis (BIA)

Question 1698

A start-up organization wants to develop a data loss prevention program (DLP). The FIRST step should be to implement:

- ☐ data encryption.
- ☐ access controls.
- ☒ data classification.
- ☐ security awareness training.

Question 1699

In a cloud technology environment, which of the following would pose the GREATESTchallenge to the investigation of security incidents?

- ☐ Data encryption
- ☒ Access to the hardware
- ☐ Compressed customer data
- ☐ Non-standard event logs

Licensed to Berend Post berend.post@it-university.nl

Question 1700

Which of the following is a general operating system access control function?

- ☐ Creating database profiles
- ☐ Verifying user authorization at a field level
- ☒ Creating individual accountability
- ☐ Logging database access activities for monitoring access violation

Explanation:

Explanation:

Creating individual accountability is the function of the general operating system. Creating database profiles, verifying user authorization at a field level and logging database access activities for monitoring access violations are all database-level access control functions.

Question 1701

Which of the following should be of GREATEST concern to an IS auditor when evaluating a new system's production readiness?

- ☐ A system defect was found during user acceptance testing.
- ☐ Functional design documentation is not complete.
- ☒ Functional requirements have not been met.
- ☐ Projected benefits have not been realized.

Question 1702

A security administrator should have read-only access for which of the following?

- ☐ Router configuration
- ☐ Password policy
- ☐ Security logs
- ☒ Services/daemons configuration

Question 1703

In an IT organization where many responsibilities are shared, which of the following would be the BEST control for detecting unauthorized data changes?

- ☐ Data changes are independently reviewed by another group.
- ☐ Users are required to periodically rotate responsibilities.
- ☐ Segregation of duties conflicts are periodically reviewed.
- ☒ Data changes are logged in an outside application.

Licensed to Berend Post berend.post@it-university.nl

Question 1704

The PRIMARY responsibility of a project steering committee is to:

- ☐ ensure that each project deadline is met
- ☐ undertake final acceptance of the system for implementation
- ☐ ensure that systems developed meet business needs
- ☒ provide day-to-day guidance and oversight

Question 1705

A web application is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

- ☒ Penetration test results
- ☐ Database application monitoring logs
- ☐ Code review by a third party
- ☐ Web application firewall implementation

Question 1706

What is the BEST way for an IS auditor to address the risk associated with over-retention of personal data after identifying a large number of customer records retained beyond the retention period defined by law?

- ☒ Recommend automating deletion of records beyond the retention period.
- ☐ Schedule regular internal audits to identify records for deletion.
- ☐ Report the retention period noncompliance to the regulatory authority.
- ☐ Escalate the over-retention issue to the data privacy officer for follow-up.

Question 1707

Which of the following would MOST effectively reduce social engineering incidents?

- ☒ Security awareness training
- ☐ increased physical security measures
- ☐ E-mail monitoring policy
- ☐ intrusion detection systems

Explanation:

Explanation:

Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e- mail in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

Licensed to Berend Post berend.post@it-university.nl

Question 1708

During development of an information security policy, which of the following would BEST ensure alignment to business objectives?

- ☐ Incorporation of industry best practices
- ☐ Linkage between policy and procedures
- ☒ Use of a balanced scorecard
- ☐ Input from relevant stakeholders

Question 1709

The objective of using coding standards for systems development is to:

- ☐ facilitate program maintenance.
- ☐ facilitate user testing.
- ☒ ensure the completeness of requirements.
- ☐ ensure that business needs are met.

Question 1710

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

- ☒ Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Explanation:

Explanation:

Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

Licensed to Berend Post berend.post@it-university.nl

Question 1711

Which of the following is MOST important for successful incident response?

- ☐ The timeless of attack recognition
- ☐ The ability to trace the source of the attack
- ☐ The quantity of data logged by the attack control tools
- ☒ Blocking the attack route immediately

Question 1712

Identify the correct sequence of Business Process Reengineering (BPR) benchmarking process from the given choices below?

- ☒ PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE
- ☐ OBSERVE, PLAN, RESEACH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, OBSERVE, RESEARCH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, RESEARCH, ANALYZE, OBSERVE, ADOPT and IMPROVE

Explanation:

The correct sequence of BRP benchmarking is PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE.

For your exam you should know the information below:

Overview of Business Process Reengineering

One of the principles in business that remains constant is the need to improve your processes and procedures. Most trade magazines today contain discussions of the detailed planning necessary for implementing change in an organization. The concept of change must be accepted as a fundamental principle. Terms such as business evolution and continuous improvement ricochet around the room in business meetings. It's a fact that organizations which fail to change are destined to perish.

As a CISA, you must be prepared to investigate whether process changes within the organization are accounted for with proper documentation. All internal control frameworks require that management be held responsible for safeguarding all the assets belonging to their organization. Management is also responsible for increasing revenue.

BPR Application Steps

ISACA cites six basic steps in their general approach to BPR. These six steps are simply an extension of Stewart's Plan-Do-Check-Act model for managing projects:

Envision -Visualize a need (envision). Develop an estimate of the ROI created by the proposed change. Elaborate on the benefit with a preliminary project plan to gain sponsorship from the organization. The plan should define the areas to be reviewed and clarify the desired result at the

Licensed to Berend Post berend.post@it-university.nl

end of the project (aka end state objective). The deliverables of the envision phase include the following:

Project champion working with the steering committee to gain top management approval

Brief description of project scope, goals, and objectives description of the specific deliverables from this project with a preliminary charter to evidence management's approval, the project may proceed into the initiation phase.

Initiate -This phase involves setting BPR goals with the sponsor. Focus on planning the collection of detailed evidence necessary to build the subsequent BPR plan for redesigning the process. Deliverables in the initiation phase include the following:

Identifying internal and external requirements (project specifications)

Business case explaining why this project makes sense (justification) and the estimated return on investment compared to the total cost (net ROI)

Formal project plan with budget, schedule, staffing plan, procurement plan, deliverables, and project risk analysis

Level of authority the BPR project manager will hold and the composition of any support committee or task force that will be required

From the profit and loss (P&L) statement, identify the item line number that money will be debited from to pay for this project and identify the specific P&L line number that the financial return will later appear under (to provide strict monitoring of the ROI performance)

Formal project charter signed by the sponsors It's important to realize that some BPR projects will proceed to their planned conclusion and others may be halted because of insufficient evidence. After a plan is formally approved, the

BPR project may proceed to the diagnostic phase.

Diagnose Document existing processes. Now it's time to see what is working and identify the source of each requirement. Each process step is reviewed to calculate the value it creates. The goal of the diagnostic phase is to gain a better understanding of existing processes. The data collected in the diagnostic phase forms the basis of all planning decisions:

Detailed documentation of the existing process

Performance measurement of individual steps in the process

Evidence of specific process steps that add customer value

Identification of process steps that don't add value

Definition of attributes that create value and quality

Put in the extra effort to do a good job of collecting and analyzing the evidence. All future assumptions will be based on evidence from the diagnostic phase.

Licensed to Berend Post berend.post@it-university.nl

Redesign- Using the evidence from the diagnostic phase, it's time to develop the new process.

This will take several planning iterations to ensure that the strategic objectives are met. The formal redesign plans will be reviewed by sponsors and stakeholders. A final plan will be presented to the steering committee for approval. Here's an example of deliverables from the redesign phase.

Comparison of the envisioned objective to actual specifications

Analysis of alternatives (AoA)

Prototyping and testing of the redesigned process

Formal documentation of the final design

The project will need formal approval to proceed into the reconstruction phase. Otherwise, the redesign is halted pending further scrutiny while comparing the proposed design with available evidence. Insufficient evidence warrants halting the project.

Reconstruct With formal approval received, it's time to begin the implementation phase.

The current processes are deconstructed and reassembled according to the plan. Reconstruction may be in the form of a parallel process, modular changes, or complete transition. Each method presents a unique risk and reward opportunity. Deliverables from this phase include the following:

Conversion plan with dependencies in time sequence

Change control management

Execution of conversion plan with progress monitoring

Training of users and support personnel

Pilot implementation to ensure a smooth migration Formal approval by the sponsor.

The reconstructed process must be formally approved by management to witness their consent for fitness of use. IT governance dictates that executive management shall be held responsible for any failures and receive recognition for exceptional results. System performance will be evaluated again after entering production use.

Evaluate (post evaluation) The reconstructed process is monitored to ensure that it works and is producing the strategic value as forecast in the original justification.

Comparison of original forecast to actual performance Identification of lessons learned

Total quality management plan to maintain the new process

A method of continuous improvement is implemented to track the original goals against actual process performance. Annual reevaluation is needed to adapt new requirements or new opportunities.

Benchmarking as a BPR Tool

Licensed to Berend Post berend.post@it-university.nl

Benchmarking is the process of comparing performance data (aka metrics). It can be used to evaluate business processes that are under consideration for reengineering. Performance data may be obtained by using a self-assessment or by auditing for compliance against a standard (reference standard). Evidence captured during the diagnostic phase is considered the key to identifying areas for performance improvement and documenting obstacles. ISACA offers the following general guidelines for performing benchmarks:

Plan Identify the critical processes and create measurement techniques to grade the processes.

Research Use information about the process and collect regular data (samples) to build a baseline for comparison. Consider input from your customers and use analogous data from other industries.

Observe Gather internal data and external data from a benchmark partner to aid the comparison results. Benchmark data can also be compared against published standards.

Analyze Look for root cause-effect relationships and other dependencies in the process. Use predefined tools and procedures to collate the data collected from all available sources.

Adapt Translate the findings into hypotheses of how these findings will help or hurt strategic business goals. Design a pilot test to prove or disprove the hypotheses.

Improve Implement a prototype of the new processes. Study the impact and note any unexpected results. Revise the process by using controlled change management. Measure the process results again. Use reestablished procedures such as total quality management for continuous improvement.

The following answers are incorrect:

The other options specified does not represent the correct sequence of BRP benchmarking steps.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 219 to 211

CISA certified information system auditor study guide Second Edition Page Number 154 to 158

Licensed to Berend Post berend.post@it-university.nl

Question 1713

Which of the following processes are performed during the design phase of the systems development life cycle (SDLC) model?

- ☐ Develop test plans.
- ☒ Baseline procedures to prevent scope creep.
- ☐ Define the need that requires resolution, and map to the major requirements of the solution.
- ☐ Program and test the new system. The tests verify and validate what has been developed.

Explanation:

Explanation:

Procedures to prevent scope creep are baselined in the design phase of the systems- development life cycle (SDLC) model.

Question 1714

Which of the following is MOST important for an IS auditor to ensure is included in a global organization's online data privacy notification to customers?

- ☐ Consequences to the organization for mishandling the data
- ☒ Consent terms including the purpose of data collection
- ☐ Contact information for reporting violations of consent
- ☐ Industry standards for data breach notification

Question 1715

What is often assured through table link verification and reference checks?

- ☒ Database integrity
- ☐ Database synchronization
- ☐ Database normalcy
- ☐ Database accuracy

Explanation:

Explanation:

Database integrity is most often ensured through table link verification and reference checks.

Licensed to Berend Post berend.post@it-university.nl

Question 1716

Network ILD&P are typically installed:

- ☐ on the organization's internal network connection.
- ☒ on the organization's internet network connection.
- ☐ on each end user stations.
- ☐ on the firewall.
- ☐ None of the choices.

Explanation:

Explanation:

Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

Question 1717

The MOST likely explanation for a successful social engineering attack is:

- ☐ that computers make logic errors.
- ☒ that people make judgment errors.
- ☐ the computer knowledge of the attackers.
- ☐ the technological sophistication of the attack method.

Explanation:

Explanation:

Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

Question 1718

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

- ☐ Overall number of users supported
- ☒ Percentage of incidents solved in the first call
- ☐ Number of incidents reported to the help desk
- ☐ Number of agents answering the phones

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C and D are not quality measures of the help desk service.

Question 1719

Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

- ☐ Employees are not required to sign a non-compete agreement.
- ☐ Security education and awareness workshops have not been completed.
- ☒ Users lack technical knowledge related to security and data protection.
- ☐ Desktop passwords do not require special characters.

Question 1720

Which of the following are used in a firewall to protect the entity's internal resources?

- ☒ Internet Protocol (IP) address restrictions
- ☐ Remote access servers
- ☐ Secure Sockets Layers (SSLs)
- ☐ Fail-over services

Question 1721

Which of the following is the BEST methodology to use for estimating the complexity of developing a large business application?

- ☒ Function point analysis
- ☐ Software cost estimation
- ☐ Work breakdown structure
- ☐ Critical path analysis

Question 1722

Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?

- ☒ Achieve standards alignment through an increase of resources devoted to the project
- ☐ Align the data definition standards after completion of the project
- ☐ Delay the project until compliance with standards can be achieved
- ☐ Enforce standard compliance by adopting punitive measures against violators

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Provided that data architecture, technical, and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources. The usage of nonstandard data definitions would lower the efficiency of the new development, and increase the risk of errors in critical business decisions. To change data definition standards after project conclusion (choice B) is risky and is not a viable solution. On the other hand, punishing the violators (choice D) or delaying the project (choice C) would be an inappropriate suggestion because of the likely damage to the entire project profitability.

Question 1723

Which of the following is the MOST effective way for an organization to ensure its third-party service providers are aware of information security requirements and expectations?

- ☐ Providing information security training to third-party personnel
- ☐ Auditing the service delivery of third-party providers
- ☒ Inducting information security clauses within contracts
- ☐ Requiring third parties to sign confidentiality agreements

Question 1724

Which of the following layer in in an enterprise data flow architecture is directly death with by end user with information?

- ☒ Desktop access layer
- ☐ Data preparation layer
- ☐ Data mart layer
- ☐ Data access layer

Explanation:

Presentation/desktop access layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

Licensed to Berend Post berend.post@it-university.nl

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Licensed to Berend Post berend.post@it-university.nl

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Licensed to Berend Post berend.post@it-university.nl

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Data mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 1725

An IS auditor is reviewing a contract for the outsourcing of IT facilities. If missing, which of the following should present the GREATEST concern to the auditor?

- ☐ Access control requirements
- ☐ Hardware configurations
- ☒ Perimeter network security diagram
- ☐ Help desk availability

Licensed to Berend Post berend.post@it-university.nl

Question 1726

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- ☐ the IT infrastructure.
- ☐ organizational policies, standards and procedures.
- ☒ legal and regulatory requirements.
- ☐ the adherence to organizational policies, standards and procedures.

Explanation:

Explanation:

To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

Question 1727

An organization has been recently downsized, in light of this, an IS auditor decides to test logical access controls. The IS auditor's PRIMARY concern should be that:

- ☒ all system access is authorized and appropriate for an individual's role and responsibilities.
- ☐ management has authorized appropriate access for all newly-hired individuals.
- ☐ only the system administrator has authority to grant or modify access to individuals.
- ☐ access authorization forms are used to grant or modify access to individuals.

Explanation:

Explanation:

The downsizing of an organization implies a large number of personnel actions over a relatively short period of time. Employees can be assigned new duties while retaining some or all of their former duties. Numerous employees may be laid off. The auditor should be concerned that an appropriate segregation of duties is maintained, that access is limited to what is required for an employee's role and responsibilities, and that access is revoked for those that are no longer employed by the organization. Choices B, C and D are all potential concerns of an IS auditor, but in light of the particular risks associated with a downsizing, should not be the primary concern.

Licensed to Berend Post berend.post@it-university.nl

Question 1728

The GREATEST benefit of risk-based auditing is that it:

- ☐ demonstrates compliance with regulatory requirements.
- ☐ enables alignment of resources to significant risk areas.
- ☐ allows an organization to identify and eliminate low-risk areas.
- ☒ identifies problem areas within an organization.

Question 1729

At what point in software development should the user acceptance test plan be prepared?

- ☒ Implementation planning
- ☐ Requirements definition
- ☐ Transfer into production
- ☐ Feasibility study

Question 1730

During an audit of a financial application, it was determined that many terminated users' accounts were not disabled. Which of the following should be the IS auditor's NEXT step?

- ☒ Perform a review of terminated users' account activity.
- ☐ Conclude that IT general controls are ineffective.
- ☐ Communicate risks to the application owner.
- ☐ Perform substantive testing of terminated users' access rights.

Question 1731

What are trojan horse programs?

- ☐ A common form of internal attack
- ☐ Malicious programs that require the aid of a carrier program such as email
- ☐ Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
- ☒ A common form of Internet attack

Explanation:

Explanation: Trojan horse programs are a common form of Internet attack.

Licensed to Berend Post berend.post@it-university.nl

Question 1732

Which of the following would be MOST helpful in ensuring security procedures are followed by employees in a multinational organization?

- ☐ Security architecture review
- ☐ Regular clean desk reviews
- ☒ Comprehensive end-user training
- ☐ Regular policy updates by management

Question 1733

Which of the following is the MOST significant concern when backup tapes are encrypted?

- ☒ Loss of the encryption key
- ☐ Lack of physical security over the tapes
- ☐ Incompatibility with future software versions
- ☐ Inaccurate data due to encryption processing

Question 1734

An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control BESTmitigate?

- ☐ Customer discounts not being applied
- ☒ A legitimate transaction being paid multiple times
- ☐ Invalid payments being processed by the system
- ☐ Delay of purchase orders

Question 1735

Which of the following controls BEST ensures appropriate segregation of duties within an accounts payable department?

- ☐ Ensuring that audit trails exist for transactions
- ☐ Restricting access to update programs to accounts payable staff only
- ☒ Restricting program functionality according to user security profiles
- ☐ Including the creator's user ID as a field in every transaction record created

Licensed to Berend Post berend.post@it-university.nl

Question 1736

An IS auditor is conducting a pre-implementation review to determine a new system's production readiness. The auditor's PRIMARY concern should be whether:

- ☐ the project adhered to the budget and target date
- ☐ users were involved in the quality assurance (QA) testing
- ☒ there are unresolved high-risk items
- ☐ benefits realization has been evidenced

Question 1737

Which of the following is an advantage of decentralized security administration?

- ☐ Greater integrity
- ☒ Faster turnaround
- ☐ More uniformity
- ☐ Better-trained administrators

Question 1738

The PRIMARY benefit of integrating information security activities into change management processes is to:

- ☐ protect the organization from unauthorized changes.
- ☒ ensure required controls are included in changes.
- ☐ provide greater accountability for security-related changes in the business.
- ☐ protect the business from collusion and compliance threats.

Question 1739

The effectiveness of an incident response team will be GREATEST when:

- ☒ the incident response process is updated based on lessons learned
- ☐ incidents are identified using a security information and event monitoring (SIEM) system
- ☐ the incident response team members are trained security personnel
- ☐ the incident response team meets on a regular basis to review log files

Question 1740

Which of the following is the MOST effective control to minimize the risk of cross-site scripting (XSS)?

- ☒ Periodic vulnerability assessments
- ☐ Secure coding practices
- ☐ Network intrusion prevention system
- ☐ Web firewall policy

Licensed to Berend Post berend.post@it-university.nl

Question 1741

An IT organization's incident response plan is which type of control?

- ☐ Preventive
- ☒ Corrective
- ☐ Detective
- ☐ Directive

Question 1742

Which of the following is the BEST method to prevent wire transfer fraud by bank employees?

- ☐ Re-keying of wire dollar amounts
- ☐ Independent reconciliation
- ☐ Two-factor authentication control
- ☒ System-enforced dual control

Question 1743

An IS auditor performing an application maintenance audit would review the log of program changes for the:

- ☒ authorization of program changes.
- ☐ creation date of a current object module.
- ☐ number of program changes actually made.
- ☐ creation date of a current source program.

Explanation:

Explanation:

The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

Question 1744

In which of the following cloud computing service model are applications hosted by the service provider and made available to the customers over a network?

- ☒ Software as a service
- ☐ Data as a service
- ☐ Platform as a service
- ☐ Infrastructure as a service

Explanation:

Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

Licensed to Berend Post berend.post@it-university.nl

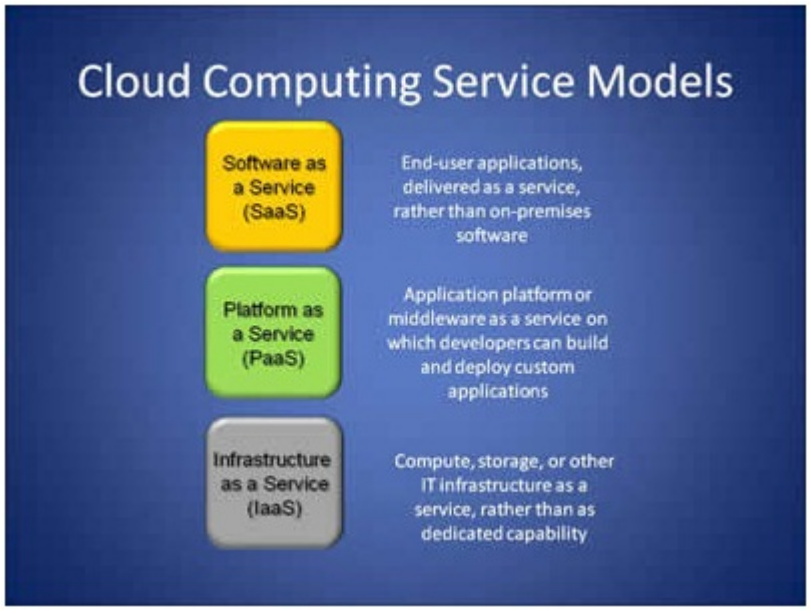
Seas is closely related to the ASP (application service provider) and on demand computing software delivery models.

For your exam you should know below information about Cloud Computing:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud computing service model

Cloud computing service models



Software as a Service (Seas)

Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for Seas. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for Seas distribution.

Licensed to Berend Post berend.post@it-university.nl

Provider gives users access to specific application software (CRM, e-mail, games). The provider gives the customers network based access to a single copy of an application created specifically for Seas distribution and use.

Benefits of the Seas model include:

easier administration

automatic updates and patch management

compatibility: All users will have the same version of software.

easier collaboration, for the same reason

global accessibility.

Platform as a Service (Peas)

Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Cloud providers deliver a computing platform, which can include an operating system, database, and web server as a holistic execution environment. Where Iasi is the “raw IT network,” Peas is the software environment that runs on top of the IT network.

Platform as a Service (Peas) is an outgrowth of Software as a Service (Seas), a software distribution model in which hosted software applications are made available to customers over the Internet. Peas has several advantages for developers. With Peas, operating system features can be changed and upgraded frequently. Geographically distributed development teams can work together on software development projects. Services can be obtained from diverse sources that cross international boundaries. Initial and ongoing costs can be reduced by the use of infrastructure services from a single vendor rather than maintaining multiple hardware facilities that often perform duplicate functions or suffer from incompatibility problems. Overall expenses can also be minimized by unification of programming development efforts.

On the downside, Peas involves some risk of "lock-in" if offerings require proprietary service interfaces or development languages. Another potential pitfall is that the flexibility of offerings may not meet the needs of some users whose requirements rapidly evolve.

Infrastructure as a Service (Iasi)

Licensed to Berend Post berend.post@it-university.nl

Cloud providers offer the infrastructure environment of a traditional data center in an on-demand delivery method. Companies deploy their own operating systems, applications, and software onto this provided infrastructure and are responsible for maintaining them.

Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.

Platform as a service - Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Infrastructure as a service - Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689

http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service

http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS

http://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

Licensed to Berend Post berend.post@it-university.nl

Question 1745

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

- ☐ Signature-based
- ☒ Neural networks-based
- ☐ Statistical-based
- ☐ Host-based

Explanation:

Explanation:

The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning. Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

Question 1746

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- ☒ Accountability for the corporate security policy
- ☐ Defining the corporate security policy
- ☐ Implementing the corporate security policy
- ☐ Defining security procedures and guidelines

Explanation:

Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

Question 1747

What would be the major purpose of rootkit?

- ☒ to hide evidence from system administrators.
- ☐ to encrypt files for system administrators.
- ☐ to corrupt files for system administrators.
- ☐ to hijack system sessions.
- ☐ None of the choices.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

rootkit originally describes those recompiled Unix tools that would hide any trace of the intruder.

You can say that the only purpose of rootkit is to hide evidence from system administrators so there is no way to detect malicious special privilege access attempts.

Question 1748

A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

- ☒ Verifying production to customer orders
- ☐ Logging all customer orders in the ERP system
- ☐ Using hash totals in the order transmitting process
- ☐ Approving (production supervisor) orders prior to production

Explanation:

Explanation:

Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processing centrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

Question 1749

Documentation of a business case used in an IT development project should be retained until:

- ☒ the end of the system's life cycle.
- ☐ the project is approved.
- ☐ user acceptance of the system.
- ☐ the system is in production.

Explanation:

Explanation:

A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates vs. actuals. Questions like, 'why do we do that', 'What was the original intent' and 'how did we perform against the plan' can be answered, and lessons for developing future business cases can be learned. During the development phase of a project one should always validate the business case, as it is a good management instrument. After finishing a project and entering production, the business case and all the completed research are valuable sources of information that should be kept for further reference

Licensed to Berend Post berend.post@it-university.nl

Question 1750

Which of the following processes is the FIRST step in establishing an information security policy?

- ☐ Security controls evaluation
- ☒ Business risk assessment
- ☐ Review of current global standards
- ☐ Information security audit

Question 1751

An IS auditor examining a biometric user authentication system establishes the existence of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Of the following, which is the BEST control against this risk?

- ☒ Kerberos
- ☐ Vitality detection
- ☐ Multimodal biometrics
- ☐ Before-image/after-image logging

Explanation:

Explanation:

Kerberos is a network authentication protocol for client-server applications that can be used to restrict access to the database to authorized users. Choices B and C are incorrect because vitality detection and multimodal biometrics are controls against spoofing and mimicry attacks. Before-image/after-image logging of database transactions is a detective control, as opposed to Kerberos, which is a preventative control.

Question 1752

An accurate biometric system usually exhibits (Choose two.):

- ☒ low EER
- ☒ low CER
- ☐ high EER
- ☐ high CER
- ☐ None of the choices.

Explanation:

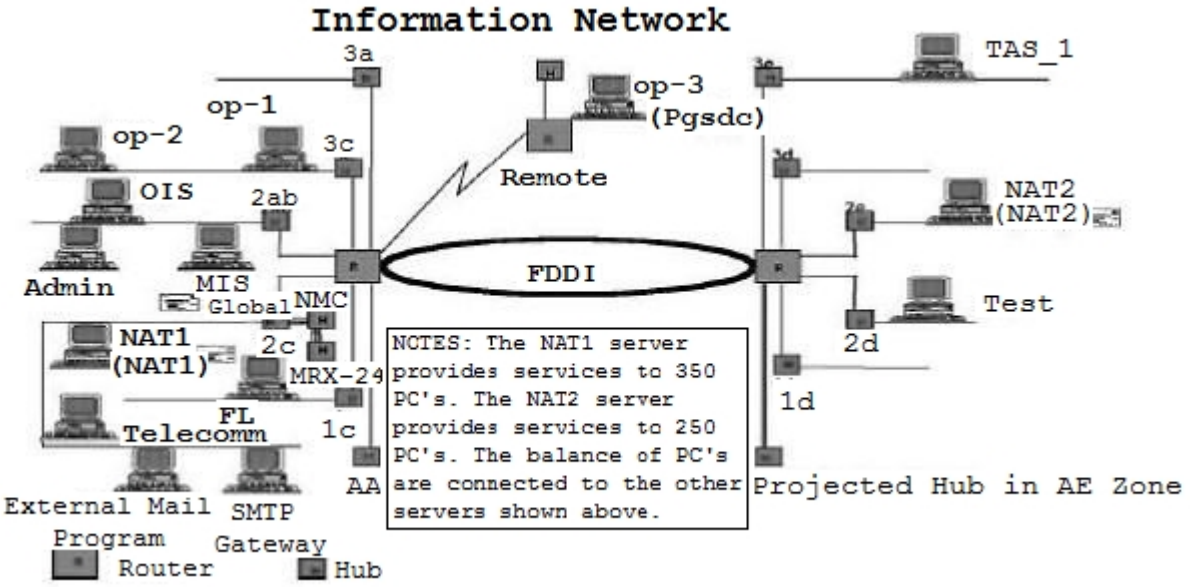
Explanation:

One most commonly used measure of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

Licensed to Berend Post berend.post@it-university.nl

Question 1753

For locations 3a, 1d and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?



- ☐ Intelligent hub
- ☐ Physical security over the hubs
- ☒ Physical security and an intelligent hub
- ☐ No controls are necessary since this is not a weakness

Explanation:

Explanation:

Open hubs represent a significant control weakness because of the potential to access a network connection easily. An intelligent hub would allow the deactivation of a single port while leaving the remaining ports active. Additionally, physical security would also provide reasonable protection over hubs with active ports.

Question 1754

To confirm integrity for a hashed message, the receiver should use:

- ☐ a different hashing algorithm from the sender's to create a numerical representation of the file.
- ☐ a different hashing algorithm from the sender's to create a binary image of the file.
- ☐ the same hashing algorithm as the sender's to create a binary image of the file.
- ☒ the same hashing algorithm as the sender's to create a numerical representation of the file.

Licensed to Berend Post berend.post@it-university.nl

Question 1755

An IS auditor is assessing an organization's data loss prevention (DLP) solution for protecting intellectual property from insider theft. Which of the following would the auditor consider MOST important for effective data protection?

- ☐ Employee training on information handling
- ☒ Creation of DLP policies and procedures
- ☐ Encryption of data copied to flash drives
- ☐ Identification and classification of sensitive data

Question 1756

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

- ☒ Presence of spyware in one of the ends
- ☐ The use of a traffic sniffing tool
- ☐ The implementation of an RSA-compliant solution
- ☐ A symmetric cryptography is used for transmitting data

Explanation:

Explanation:

Encryption using secure sockets layer/transport layer security (SSL/TLS) tunnels makes it difficult to intercept data in transit, but when spyware is running on an end user's computer, data are collected before encryption takes place. The other choices are related to encrypting the traffic, but the presence of spyware in one of the ends captures the data before encryption takes place.

Question 1757

A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

- ☐ Unit testing
- ☒ Integration testing
- ☐ Design walk-throughs
- ☐ Configuration management

Explanation:

Explanation:

A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight), units are tested by the programmer, and then transferred to the acceptance test area. This often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

Licensed to Berend Post berend.post@it-university.nl

Question 1758

The 'trusted systems' approach has been predominant in the design of:

- ☒ many earlier Microsoft OS products
- ☐ the IBM AS/400 series
- ☐ the SUN Solaris series
- ☐ most OS products in the market
- ☐ None of the choices.

Explanation:

Explanation:

The 'trusted systems' approach has been predominant in the design of many Microsoft OS products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use'.

Question 1759

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

- ☐ Parallel
- ☐ Preparedness
- ☒ Walk-thorough
- ☐ Paper

Explanation:

Explanation:

Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

Question 1760

Which of the following must exist to ensure the viability of a duplicate information processing facility?

- ☐ The site is near the primary site to ensure quick and efficient recovery.
- ☐ The site contains the most advanced hardware available.
- ☒ The workload of the primary site is monitored to ensure adequate backup is available.
- ☐ The hardware is tested when it is installed to ensure it is working properly.

Explanation:

Explanation:

Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not

Licensed to Berend Post berend.post@it-university.nl

adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

Question 1761

Which of the following is the GREATEST security risk associated with data migration from a legacy HR system to a cloud-based system?

- ☐ System performance may be impacted by the migration.
- ☐ Records past their retention period may not be migrated to the new system.
- ☐ Data from the source and target system may have different data formats.
- ☒ Data from the source and target system may be intercepted.

Question 1762

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

- ☐ The use of diskless workstations
- ☒ Periodic checking of hard drives
- ☐ The use of current antivirus software
- ☐ policies that result in instant dismissal if violated

Explanation:

Explanation:

The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

Question 1763

Which of the following would BEST provide an information security manager with sufficient assurance that a service provider complies with organization's information security requirements?

- ☐ A live demonstration of the third-party supplier's security capabilities
- ☐ Third-party security control self-assessment results
- ☒ An independent review report indicating compliance with industry standards
- ☐ The ability to audit the third-party supplier's IT systems and processes

Licensed to Berend Post berend.post@it-university.nl

Question 1764

Which of the following should be included in a feasibility study for a project to implement an EDI process?

- ☐ The encryption algorithm format
- ☐ The detailed internal control procedures
- ☒ The necessary communication protocols
- ☐ The proposed trusted third-party agreement

Explanation:

Explanation:

Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as there may be significant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.

Question 1765

The performance of an order-processing system can be measured MOST reliably by monitoring:

- ☒ input/request queue length.
- ☐ turnaround time of completed transactions.
- ☐ application and database servers' CPU load.
- ☐ heartbeats between server systems.

Question 1766

Minimum password length and password complexity verification are examples of:

- ☐ detection controls.
- ☐ control objectives.
- ☐ audit objectives.
- ☒ control procedures.

Explanation:

Explanation:

Control procedures are practices established by management to achieve specific control objectives. Password controls are preventive controls, not detective controls. Control objectives are declarations of expected results from implementing controls and audit objectives are the specific goals of an audit.

Licensed to Berend Post berend.post@it-university.nl

Question 1767

Which of the following should be the PRIMARY consideration when developing an IT strategy?

- ☐ IT key performance indicators based on business objectives
- ☒ Alignment with overall business objectives
- ☐ Alignment with the IT investment portfolio
- ☐ Short and long-term plans for the enterprise IT architecture

Question 1768

During an incident management audit, an IS auditor finds that several similar incidents were logged during the audit period. Which of the following is the auditor's MOST important course of action?

- ☐ Document the finding and present it to management.
- ☐ Determine if a root cause analysis was conducted.
- ☒ Validate whether all incidents have been actioned.
- ☐ Confirm the resolution time of the incidents.

Question 1769

Overall responsibility for approving logical access rights to information assets should reside with the:

- ☒ data and systems owners.
- ☐ systems delivery and operations group.
- ☐ security administrator.
- ☐ systems administrator.

Question 1770

Which of the following type of testing validate functioning of the application under test with other system, where a set of data is transferred from one system to another?

- ☒ Interface testing
- ☐ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Explanation:

Interface or integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

For CISA exam you should know below types of testing:

Licensed to Berend Post berend.post@it-university.nl

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the systems ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.

QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the

Licensed to Berend Post berend.post@it-university.nl

application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include:

Definition of test strategies and procedure.

Design of test cases and scenarios

Execution of the tests.

Utilization of the result to verify system readiness.

Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensures internal operation of the programs according to the specification.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team.

Final Acceptance Testing – During this testing phase the defined methods of testing to apply should be incorporated into the organization's QA methodology.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 166

Licensed to Berend Post berend.post@it-university.nl

Question 1771

Which of the following attack is also known as Time of Check(TOC)/Time of Use(TOU)?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☒ Race Condition

Explanation:

A Race Condition attack is also known as Time of Check(TOC)/Time of Use(TOU).

A race condition is when processes carry out their tasks on a shared resource in an incorrect order. A race condition is possible when two or more processes use a shared resource, as in data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result will be much different than if process1 carried out its tasks on the data before process 2.

In software, when the authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the authorization step to be completed before the authentication step. This would be a flaw in the software that the attacker has figured out how to exploit. A race condition occurs when two or more processes use the same resource and the sequences of steps within the software can be carried out in an improper order, something that can drastically affect the output. So, an attacker can force the authorization step to take place before the authentication step and gain unauthorized access to a resource.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access

Licensed to Berend Post berend.post@it-university.nl

identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cyber crime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 324

Official ISC2 guide to CISSP CBK 3rd Edition Page number 66

CISSP All-In-One Exam guide 6th Edition Page Number 161

Question 1772

When an information security manager presents an information security program status report to senior management, the MAIN focus should be:

- ☒ key performance indicators (KPIs)
- ☐ critical risks indicators
- ☐ net present value (NPV)
- ☐ key controls evaluation

Question 1773

Off-site data backup and storage should be geographically separated so as to _____ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

- ☐ Accept
- ☐ Eliminate
- ☐ Transfer
- ☒ Mitigate

Explanation:

Explanation:

Off-site data backup and storage should be geographically separated, to mitigate the risk of a widespread physical disaster such as a hurricane or an earthquake.

Licensed to Berend Post berend.post@it-university.nl

Question 1774

Squid is an example of:

- ☐ IDS
- ☒ caching proxy
- ☐ security proxy
- ☐ connection proxy
- ☐ dialer
- ☐ None of the choices.

Explanation:

Explanation:

Squid is an example of a caching proxy, not a security proxy. It has the main purpose of locally storing copies of web pages that are popular, with the benefit of saving bandwidth.

Question 1775

An organization has detected sensitive data leakage caused by an employee of a third-party contractor. What is the BEST course of action to address this issue?

- ☐ Include security requirements in outsourcing contracts.
- ☒ Activate the organization's incident response plan.
- ☐ Limit access to the third-party contractor.
- ☐ Terminate the agreement with the third-party contractor.

Question 1776

Which of the following is the BEST reason for delaying the application of a critical security patch?

- ☐ Lack of vulnerability management
- ☐ Conflicts with software development life cycle
- ☒ Technology interdependencies
- ☐ Resource limitations

Question 1777

Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack encrypted data at rest?

- ☐ Use of symmetric encryption
- ☐ Use of asymmetric encryption
- ☐ Random key generation
- ☒ Short key length

Licensed to Berend Post berend.post@it-university.nl

Question 1778

Loading of illegal software packages onto a network by an employee is MOST effectively detected by:

- ☐ diskless workstations.
- ☒ regular scanning of hard drives
- ☐ maintaining current antivirus software.
- ☐ logging of activity on network drives.

Question 1779

A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

- ☐ Dump the volatile storage data to a disk.
- ☐ Run the server in a fail-safe mode.
- ☒ Disconnect the web server from the network.
- ☐ Shut down the web server.

Explanation:

Explanation:

The first action is to disconnect the web server from the network to contain the damage and prevent more actions by the attacker. Dumping the volatile storage data to a disk may be used at the investigation stage but does not contain an attack in progress. To run the server in a fail-safe mode, the server needs to be shut down. Shutting down the server could potentially erase information that might be needed for a forensic investigation or to develop a strategy to prevent future similar attacks.

Question 1780

Which of the following reports should an IS auditor use to check compliance with a service level agreements (SLA) requirement for uptime?

- ☐ Utilization reports
- ☐ Hardware error reports
- ☐ System logs
- ☒ Availability reports

Explanation:

Explanation:

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

Licensed to Berend Post berend.post@it-university.nl

Question 1781

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

- ☐ a lack of investment in technology.
- ☐ a lack of a methodology for systems development.
- ☒ technology not aligning with the organization's objectives.
- ☐ an absence of control over technology contracts.

Explanation:

Explanation:

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

Question 1782

Validated digital signatures in an e-mail software application will:

- ☒ help detect spam.
- ☐ provide confidentiality.
- ☐ add to the workload of gateway servers.
- ☐ significantly reduce available bandwidth.

Explanation:

Explanation:

Validated electronic signatures are based on qualified certificates that are created by a certification authority (CA), with the technical standards required to ensure the key can neither be forced nor reproduced in a reasonable time. Such certificates are only delivered through a registration authority (RA) after a proof of identity has been passed. Using strong signatures in e- mail traffic, nonrepudiation can be assured and a sender can be tracked. The recipient can configure their e-mail server or client to automatically delete e-mails from specific senders. For confidentiality issues, one must use encryption, not a signature, although both methods can be based on qualified certificates. Without any filters directly applied on mail gateway servers to block traffic without strong signatures, the workload will not increase. Using filters directly on a gateway server will result in an overhead less than antivirus software imposes. Digital signatures are only a few bytes in size and will not slash bandwidth. Even if gateway servers were to check CRLs, there is little overhead.

Licensed to Berend Post berend.post@it-university.nl

Question 1783

The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:

- ☒ current and target security state for the business.
- ☐ security program priorities to achieve an accepted risk level.
- ☐ assessed level of security risk at a particular point in time.
- ☐ level of compliance with internal policy.

Question 1784

The responsibilities of a disaster recovery relocation team include:

- ☐ obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
- ☐ locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
- ☐ managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
- ☒ coordinating the process of moving from the hot site to a new location or to the restored original location.

Explanation:

Explanation:

Choice A describes an offsite storage team, choice B defines a transportation team and choice C defines a salvage team.

Question 1785

An IS auditor evaluating a three-tier client/server architecture observes an issue with graphical user interface (GUI) tasks. Which layer should the auditor recommend the client address?

- ☒ Presentation layer
- ☐ Application layer
- ☐ Storage layer
- ☐ Transport layer

Licensed to Berend Post berend.post@it-university.nl

Question 1786

In which of the following SDLC phases would the IS auditor expect to find that controls have been incorporated into system specifications?

- ☐ Development
- ☒ Implementation
- ☐ Design
- ☐ Feasibility

Question 1787

The PRIMARY objective of service-level management (SLM) is to:

- ☒ define, agree, record and manage the required levels of service.
- ☐ ensure that services are managed to deliver the highest achievable level of availability.
- ☐ keep the costs associated with any service at a minimum.
- ☐ monitor and report any legal noncompliance to business management.

Explanation:

Explanation:

The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services. This does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level, since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

Question 1788

Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

- ☐ A hot site contracted and available as needed.
- ☐ A business continuity manual is available and current.
- ☐ insurance coverage is adequate and premiums are current.
- ☒ Media backups are performed on a timely basis and stored offsite.

Explanation:

Explanation:

Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

Licensed to Berend Post berend.post@it-university.nl

Question 1789

The BEST way to prevent fraudulent payments is to implement segregation of duties between payment processing and:

- ☐ requisition creation.
- ☐ vendor setup.
- ☒ payment approval.
- ☐ check creation.

Question 1790

During the extraction and transfer process of data from an application database to an enterprise data warehouse, some of the fields were not picked up in the extraction process and therefore did not end up in the data warehouse. Which of the following is the GREATEST concern with this situation?

- ☐ Costs associated with correcting the process may exceed budget
- ☒ Transaction errors may occur within the application
- ☐ Management decisions may be based on incorrect data
- ☐ Management reporting could be delayed

Question 1791

Which of the following would help determine the maturity of an information security awareness program?

- ☐ A review of the annual penetration test results
- ☐ A network vulnerability assessment
- ☐ A simulated social engineering test
- ☒ A gap assessment against an established model

Question 1792

Which of the following statement INCORRECTLY describes Asynchronous Transfer Mode (ATM) technique?

- ☐ ATM uses cell switching method
- ☐ ATM is high speed network technology used for LAN, MAN and WAN
- ☒ ATM works at session layer of an OSI model
- ☐ Data are segmented into fixed size cell of 53 bytes

Explanation:

The keyword INCORRECTLY is used within the question. You need to find out a statement which was incorrectly describe Asynchronous Transfer Mode.ATM operates at data link layer of an OSI model

For your exam you should know below information about WAN Technologies:

Licensed to Berend Post berend.post@it-university.nl

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Point-to-point protocol

X.25

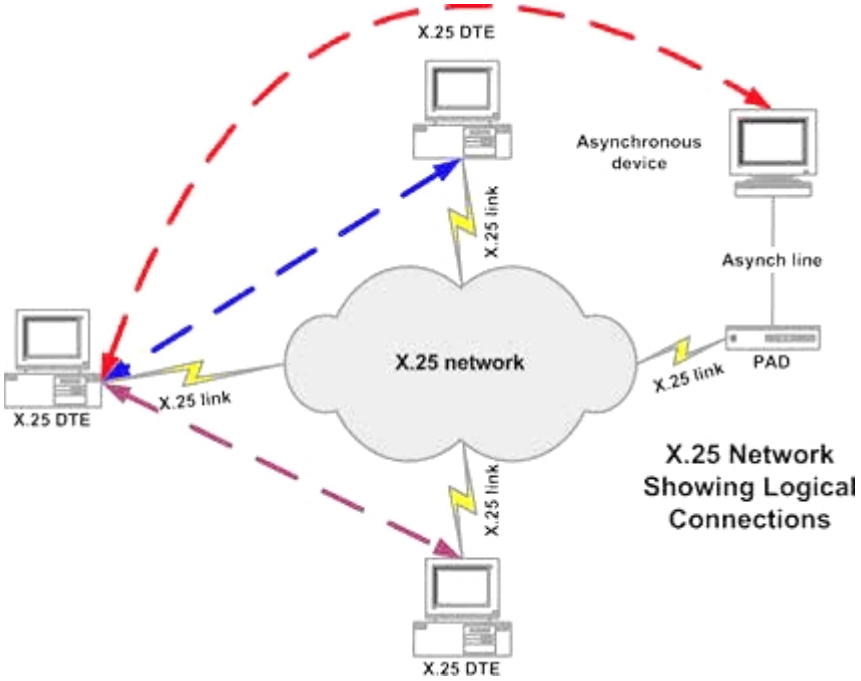
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

Licensed to Berend Post berend.post@it-university.nl



X.25

Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

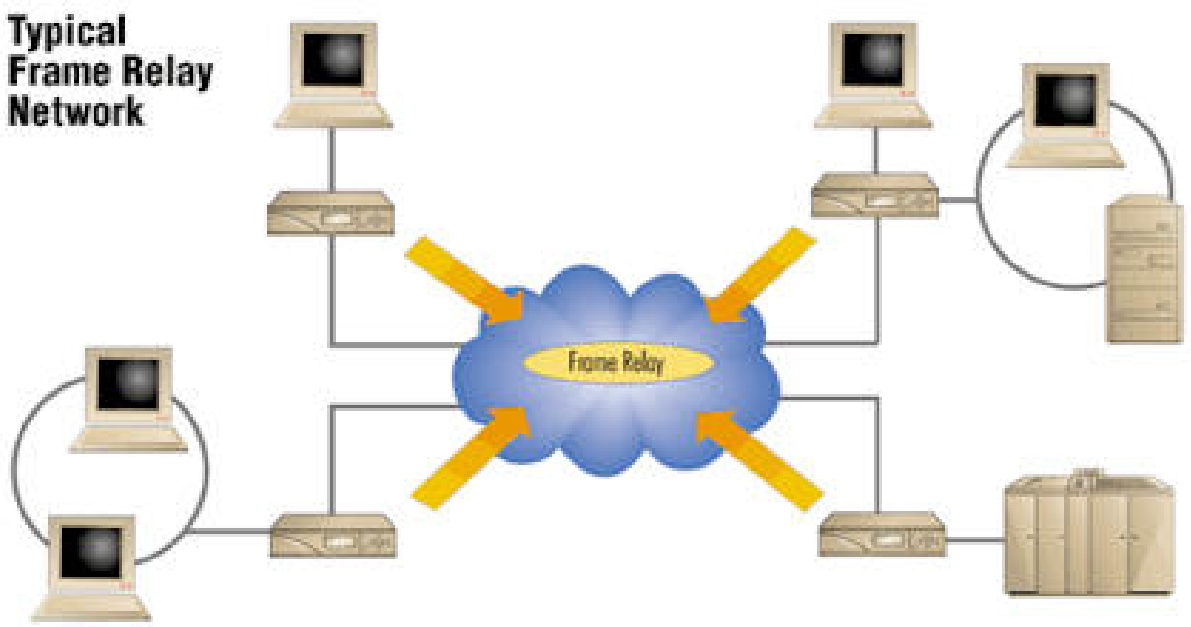
Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

Licensed to Berend Post berend.post@it-university.nl



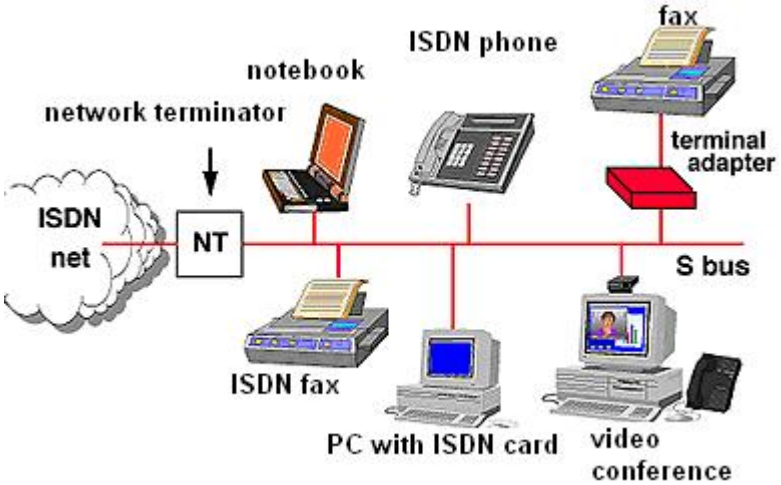
Frame Relay

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.



ISDN

Asynchronous Transfer Mode (ATM)

Licensed to Berend Post berend.post@it-university.nl

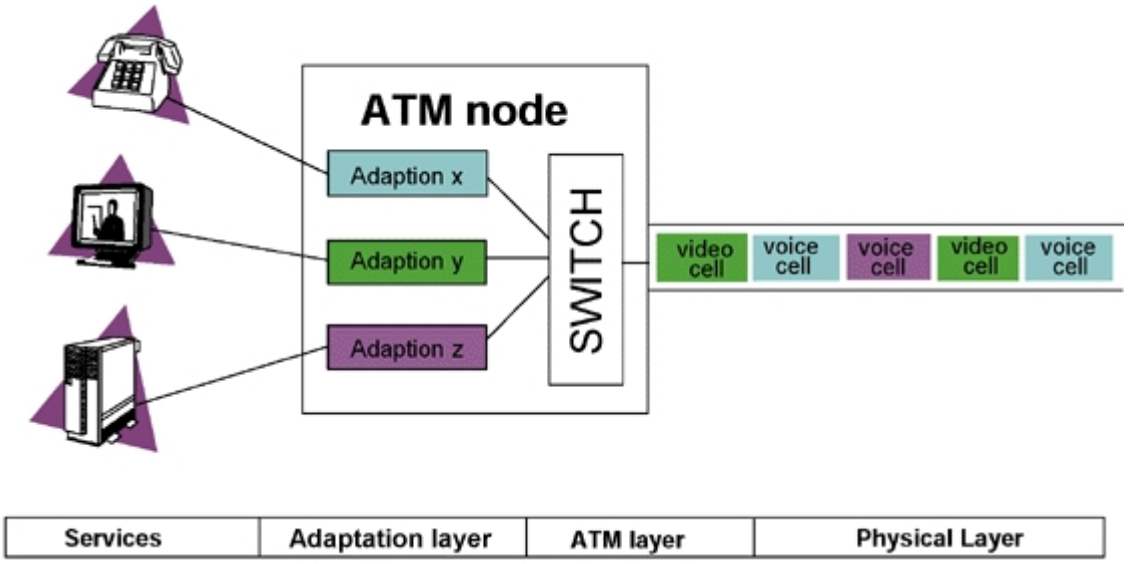
Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel

Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM



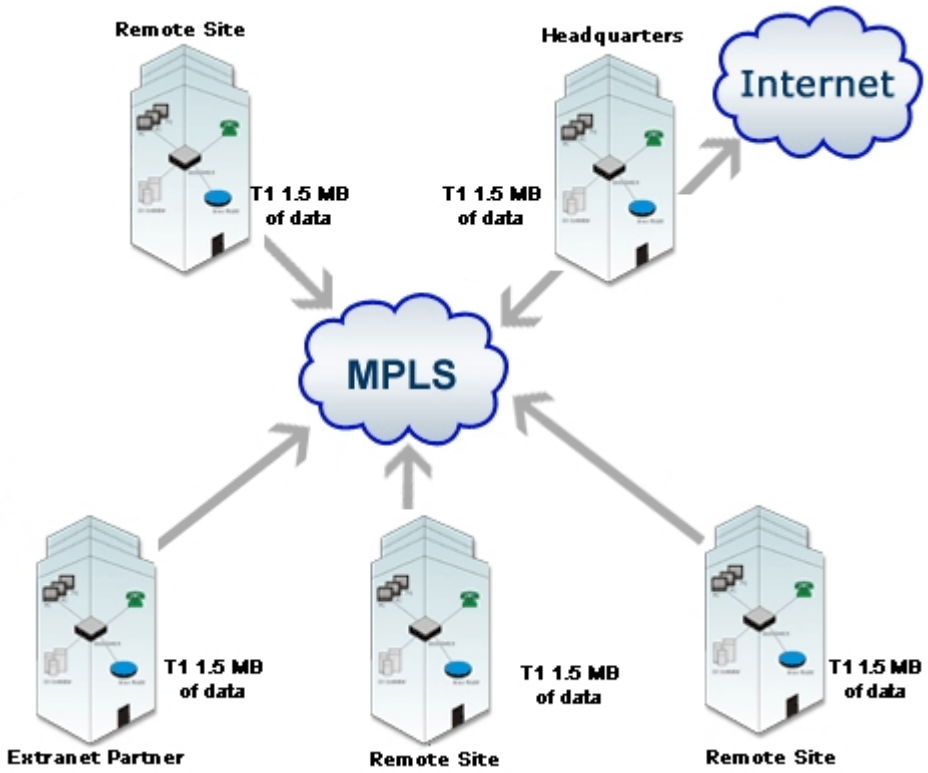
Asynchronous Transfer Mode

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS

Licensed to Berend Post berend.post@it-university.nl



The following answers are incorrect:

The other options presented correctly describes Asynchronous Transfer Mode.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

Question 1793

Which of the following should be the MOST important consideration when implementing an information security framework?

- ☒ Compliance requirements
- ☐ Audit findings
- ☐ Technical capabilities
- ☐ Risk appetite

Licensed to Berend Post berend.post@it-university.nl

Question 1794

Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

- ☐ Application layer – Telnet
- ☒ Transport layer – ICMP
- ☐ Internet layer – IP
- ☐ Network Access layer – Ethernet

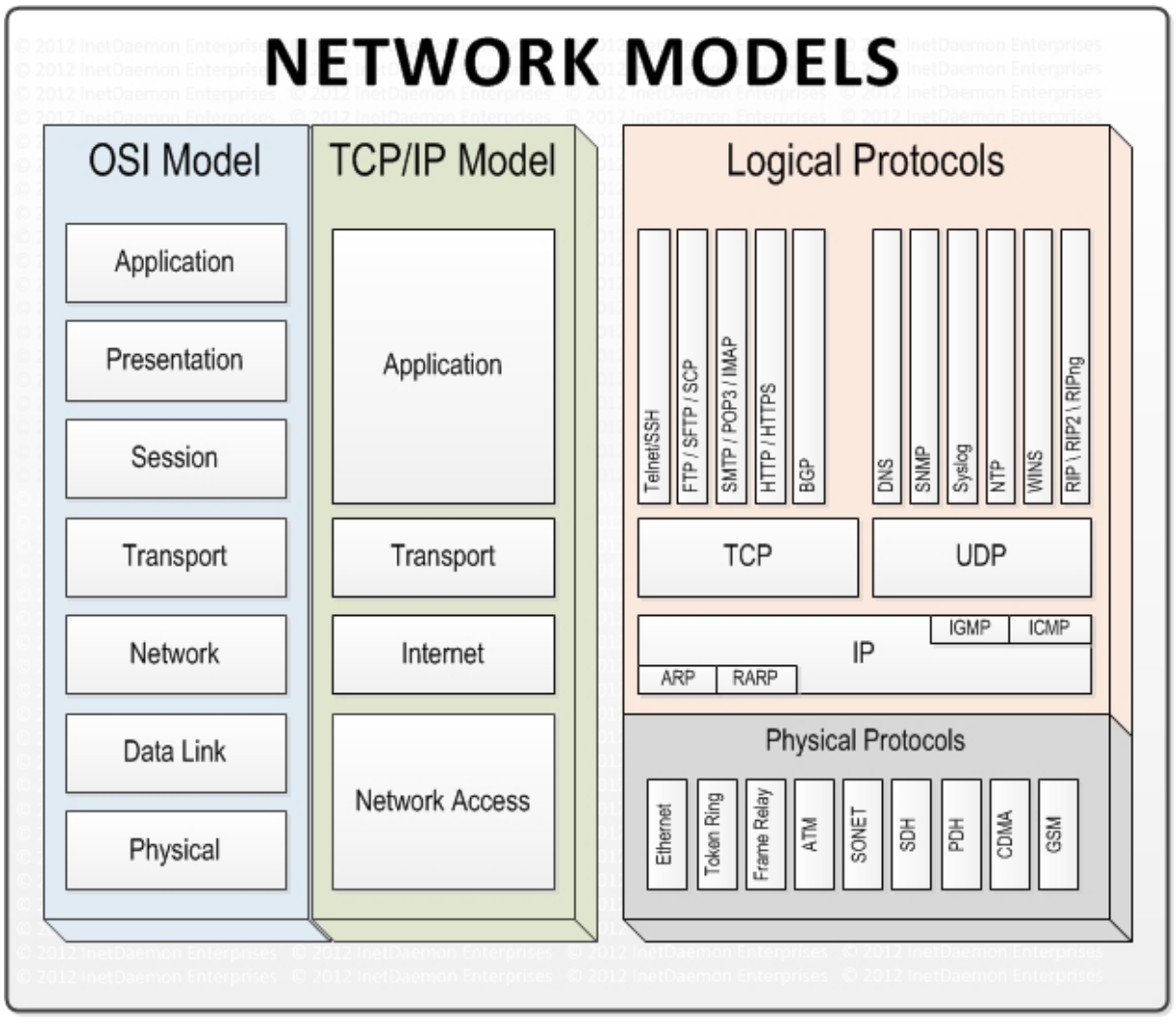
Explanation:

The keyword INCORRECT is used within the question. You need to find out the incorrect Layer to Protocol mapping.

The ICMP protocol works at Internet layer of the DoD TCP/IP model, not at the Transport Layer.

For your exam you should know below information about the TCP/IP models:

Network Models



Licensed to Berend Post berend.post@it-university.nl

Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Licensed to Berend Post berend.post@it-university.nl

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

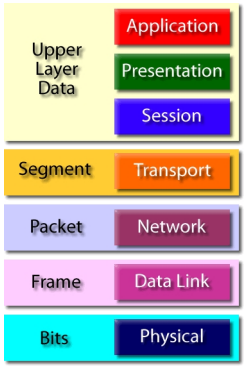
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

The other options correctly describe the Layer to Protocol mapping of the DoD TCP/IP model protocols.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 1795

To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

- ☐ examine the change control system records and trace them forward to object code files.
- ☐ review access control permissions operating within the production program libraries.
- ☒ examine object code to find instances of changes and trace them back to change control records.
- ☐ review change approved designations established within the change control system.

Explanation:

Explanation:

The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes. The other choices are valid procedures to apply in a change control audit but they do not directly address the risk of unauthorized code changes.

Question 1796

An organization has purchased a replacement mainframe computer to cope with the demands of increased business. Which of the following should be the PRIMARY concern of an IS auditor?

- ☐ The disaster recovery plan has been reviewed and updated.
- ☐ Application access controls are adequate.
- ☒ Appropriate tender evaluation processes have been followed.
- ☐ The procurement is within the planned budget for the year.

Licensed to Berend Post berend.post@it-university.nl

Question 1797

Which of the following is the PRIMARY advantage of using virtualization technology for corporate applications?

- ☒ Better utilization of resources
- ☐ Stronger data security
- ☐ Increased application performance
- ☐ Improved disaster recovery

Question 1798

With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

- ☒ clarity and simplicity of the business continuity plans.
- ☐ adequacy of the business continuity plans.
- ☐ effectiveness of the business continuity plans.
- ☐ ability of IS and end-user personnel to respond effectively in emergencies.

Explanation:

Explanation:

The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards. To evaluate effectiveness, the IS auditor should review the results from previous tests. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization had implemented plans to allow for the effective response.

Question 1799

An IS auditor is planning on utilizing attribute sampling to determine the error rate for health care claims processed. Which of the following factors will cause the sample size to decrease?

- ☒ Population size increase
- ☐ Expected error rate increase
- ☐ Acceptable risk level decrease
- ☐ Tolerate error rate increase

Licensed to Berend Post berend.post@it-university.nl

Question 1800

Which of the following should MOST concern an IS auditor reviewing an intrusion detection system (IDS)?

- ☒ Number of false negatives
- ☐ Number of false positives
- ☐ Legitimate traffic blocked by the system
- ☐ Reliability of IDS logs

Question 1801

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Database snapshots can provide an excellent audit trail for an IS auditor.

Question 1802

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

- ☐ conclude that the controls are inadequate.
- ☒ expand the scope to include substantive testing
- ☐ place greater reliance on previous audits.
- ☐ suspend the audit.

Explanation:

Explanation:

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

Licensed to Berend Post berend.post@it-university.nl

Question 1803

Which of the following is a rewrite of ipfwadm?

- ☒ ipchains
- ☐ iptables
- ☐ Netfilter
- ☐ ipcook
- ☐ None of the choices.

Explanation:

Explanation:

ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above. Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

Question 1804

The performance, risks, and capabilities of an IT infrastructure are BEST measured using a:

- ☒ balanced scorecard.
- ☐ risk management review.
- ☐ service level agreement (SLA).
- ☐ control self-assessment (CSA).

Question 1805

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

Licensed to Berend Post berend.post@it-university.nl

Question 1806

An auditor is creating an audit program in which the objective is to establish the adequacy of personal data privacy controls in a payroll process. Which of the following would be MOST important to include?

- ☐ Approval of data changes
- ☐ Audit logging of administrative user activity
- ☒ Segregation of duties controls
- ☐ User access provisioning

Question 1807

An information security manager's PRIMARY objective for presenting key risks to the board of directors is to:

- ☐ re-evaluate the risk appetite.
- ☐ quantify reputational risks.
- ☐ meet information security compliance requirements.
- ☒ ensure appropriate information security governance.

Question 1808

Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

- ☒ protect the organization from viruses and nonbusiness materials.
- ☐ maximize employee performance.
- ☐ safeguard the organization's image.
- ☐ assist the organization in preventing legal issues

Explanation:

Explanation:

The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e- mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

Licensed to Berend Post berend.post@it-university.nl

Question 1809

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model outline the major process of an organization and the external parties with which business interacts?

- ☒ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☐ Entity relationship diagrams

Explanation:

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Licensed to Berend Post berend.post@it-university.nl

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Licensed to Berend Post berend.post@it-university.nl

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Context diagram -Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram – De-construct business processes.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Licensed to Berend Post berend.post@it-university.nl

Question 1810

While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:

- ☒ shadow file processing.
- ☐ electronic vaulting.
- ☐ hard-disk mirroring.
- ☐ hot-site provisioning.

Explanation:

Explanation:

In shadow file processing, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files, such as airline booking systems. Electronic vaulting electronically transmits data either to direct access storage, an optical disc or another storage medium; this is a method used by banks. Hard-disk mirroring provides redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server. A hot site is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

Question 1811

Which of the following is MOST important for an IS auditor to verify when reviewing a critical business application that requires high availability?

- ☐ Algorithms are reviewed to resolve process inefficiencies.
- ☐ Users participate in offsite business continuity testing.
- ☒ There is no single point of failure.
- ☐ Service level agreement (SLAs) are monitored.

Question 1812

Which of the following is MOST likely to be included in computer operating procedures in a large data center?

- ☒ Instructions for job scheduling
- ☐ Procedures for resequencing source code
- ☐ Procedures for utility configuration
- ☐ Guidance on setting security parameters

Licensed to Berend Post berend.post@it-university.nl

Question 1813

Which of the following would MOST likely require a business continuity plan to be invoked?

- ☐ A distributed denial of service attack on an email server
- ☐ An unauthorized visitor discovered in the data center
- ☒ An epidemic preventing staff from performing job functions
- ☐ A hacker holding personally identifiable information hostage.

Question 1814

Which of the following is the MOST important reason to periodically review data that has already been classified?

- ☐ The associated risk may change over time.
- ☐ Additional data may have been added to the inventory.
- ☐ Older data may need to be archived on removable media.
- ☒ The classification nomenclature has changed.

Question 1815

Which of the following is an IS auditor's BEST course of action upon learning that preventive controls have been replaced with detective and corrective controls?

- ☐ Report the issue to management as the risk level has increased.
- ☐ Recommend the implementation of preventive controls in addition to the other controls.
- ☐ Verify the revised controls enhance the efficiency of related business processes.
- ☒ Evaluate whether new controls manage the risk at an acceptable level.

Question 1816

An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:

- ☐ the training needs for users after applying the patch.
- ☐ any beneficial impact of the patch on the operational systems.
- ☒ delaying deployment until testing the impact of the patch.
- ☐ the necessity of advising end users of new patches.

Explanation:

Explanation:

Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1817

Management disagrees with a finding in a draft audit report and provides supporting documentation. Which of the following should be the IS auditor's NEXT course of action?

- ☐ Document management's disagreement in the final report
- ☒ Evaluate the supporting documentation
- ☐ Escalate the issue with supporting documentation to senior management
- ☐ Finalize the draft audit report without changes

Question 1818

Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Whenever business processes have been re-engineered, the IS auditor should attempt to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes.

Question 1819

Which of the following observations noted during a review of the organization's social media practices should be of MOST concern to the IS auditor?

- ☐ The organization does not require approval for social media posts.
- ☐ More than one employee is authorized to publish on social media on behalf of the organization.
- ☐ Not all employees using social media have attended the security awareness program.
- ☒ The organization does not have a documented social media policy.

Question 1820

The PRIMARY reason for using digital signatures is to ensure data:

- ☐ confidentiality.
- ☒ integrity.
- ☐ availability.
- ☐ timeliness.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Digital signatures provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered. Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

Question 1821

Which of the following is MOST important to consider when creating audit follow-up procedures?

- ☐ Whether the organization has sufficient funds to address the issue
- ☐ Whether management has determined if risk is within the organization's risk appetite
- ☒ Whether follow-up procedures would determine if identified risks have been mitigated
- ☐ Whether the auditee has allotted sufficient time for the follow-up

Question 1822

An organization has recently converted its infrastructure to a virtualized environment. The GREATEST benefit related to disaster recovery is that virtualized servers:

- ☐ reduce the time it takes to successfully create backups.
- ☒ decrease the recovery time objective (RTO).
- ☐ eliminate the manpower necessary to restore the server.
- ☐ can be recreated on similar hardware faster than restoring from backups.

Question 1823

Reviewing which of the following would provide the GREATEST input to the asset classification process:

- ☐ Risk assessment
- ☒ Sensitivity of the data
- ☐ Replacement cost of the asset
- ☐ Compliance requirements

Licensed to Berend Post berend.post@it-university.nl

Question 1824

Within a virus, which component is responsible for what the virus does to the victim file?

- ☒ the payload
- ☐ the signature
- ☐ the trigger
- ☐ the premium
- ☐ None of the choices.

Explanation:

Explanation:

"A virus typically consist of three parts, which are a mechanism that allows them to infect other files and reproduce a trigger that activates delivery of a "payload" and the payload from which the virus often gets its name. The payload is what the virus does to the victim file."

Question 1825

Which of the following is the MOST important consideration when investigating a security breach of an e-commerce application?

- ☐ Chain of custody
- ☒ Skill set of the response team
- ☐ Notifications to law enforcement
- ☐ Procedures to analyze evidence

Question 1826

In assessing the priority given to systems covered in an organization's business continuity plan (BCP), an IS auditor should FIRST:

- ☐ review results of previous business continuity plan (BCP) tests.
- ☐ review the backup and restore processes.
- ☐ verify the criteria for disaster recovery site selection.
- ☒ validate the recovery time objectives and recovery point objectives.

Question 1827

An IS auditor is reviewing an organization's network vulnerability scan results. Which of the following processes would the scan results MOST likely feed into?

- ☒ Firewall maintenance
- ☐ Patch management
- ☐ Incident response
- ☐ Traffic management

Licensed to Berend Post berend.post@it-university.nl

Question 1828

Back Orifice is an example of:

- ☐ a virus.
- ☐ a legitimate remote control software.
- ☒ a backdoor that takes the form of an installed program.
- ☐ an eavesdropper.
- ☐ None of the choices.

Explanation:

Explanation:

"A backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing ""legitimate"" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports."

Question 1829

To maintain the confidentiality of information moved between office and home on removable media, which of the following is the MOST effective control?

- ☐ Mandatory file passwords
- ☐ Security awareness training
- ☐ Digitally signed media
- ☒ Data encryption

Question 1830

A CIO has asked an IS auditor to implement several security controls for an organization's IT processes and systems. The auditor should:

- ☐ perform the assignment and future audits with due professional care.
- ☐ obtain approval from executive management for the implementation.
- ☐ refuse due to independence issues.
- ☒ communicate the conflict of interest to audit management.

Question 1831

Which of the following is the BEST way to control scope creep during application system development?

- ☐ Involve key stakeholders.
- ☒ Implement project steering committee review.
- ☐ Implement a quality management system.
- ☐ Establish key performance indicators (KPIs).

Licensed to Berend Post berend.post@it-university.nl

Question 1832

A firm is considering using biometric fingerprint identification on all PCs that access critical datA. This requires:

- ☒ that a registration process is executed for all accredited PC users.
- ☐ the full elimination of the risk of a false acceptance.
- ☐ the usage of the fingerprint reader be accessed by a separate password.
- ☐ assurance that it will be impossible to gain unauthorized access to critical data.

Explanation:

Explanation:

The fingerprints of accredited users need to be read, identified and recorded, i.e., registered, before a user may operate the system from the screened PCs. Choice B is incorrect, as the false- acceptance risk of a biometric device may be optimized, but will never be zero because this would imply an unacceptably high risk of false rejection. Choice C is incorrect, as the fingerprint device reads the token (the user's fingerprint) and does not need to be protected in itself by a password. Choice Dis incorrect because the usage of biometric protection on PCs does not guarantee that other potential security weaknesses in the system may not be exploited to access protected data.

Question 1833

Which of the following is the MOST effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

- ☐ Review the record retention register regularly to initiate data deletion.
- ☒ Build in system logic to trigger data deletion at predefined times.
- ☐ Perform a sample check of current data against the retention schedule.
- ☐ Execute all data deletions at a predefined month during the year.

Question 1834

Which of the following is a MAJOR benefit of using a wireless network?

- ☐ Faster network speed
- ☒ Stronger authentication
- ☐ Protection against eavesdropping
- ☐ Lower installation cost

Licensed to Berend Post berend.post@it-university.nl

Question 1835

Creating which of the following is how a hacker can insure his ability to return to the hacked system at will?

- ☐ rootsec
- ☐ checksum
- ☐ CRC
- ☒ backdoors
- ☐ None of the choices.

Explanation:

Explanation:

A backdoor refers to a generally undocumented means of getting into a system, mostly for programming and maintenance/troubleshooting needs. Most real world programs have backdoors. Creating backdoors is how a hacker can insure his ability to return to the hacked system at will.

Question 1836

Which of the following is the FIRST consideration when developing a data retention policy?

- ☐ Determining the backup cycle based on retention period
- ☐ Designing an infrastructure storage strategy
- ☐ Identifying the legal and contractual retention period for data
- ☒ Determining the security access privileges to the data

Question 1837

A PRIMARY advantage of involving business management in evaluating and managing information security risks is that they:

- ☐ better understand the security architecture
- ☐ better understand organizational risks
- ☒ can balance technical and business risks
- ☐ are more objective than security management

Question 1838

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- ☒ performance measurement.
- ☐ strategic alignment.
- ☐ value delivery.
- ☐ resource management.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver {process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

Question 1839

Which of the following MOST effectively provides assurance of ongoing service delivery by a vendor?

- ☐ Regular status reporting provided by the vendor
- ☐ Short incident response time by the vendor
- ☒ Pre-defined service and operational level agreements
- ☐ Regular monitoring by service management team

Question 1840

Which of the following does a lack of adequate security controls represent?

- ☐ Threat
- ☐ Asset
- ☐ Impact
- ☒ Vulnerability

Explanation:

Explanation:

The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

Licensed to Berend Post berend.post@it-university.nl

Question 1841

During a review of an application system, an IS auditor identifies automated controls designed to prevent the entry of duplicate transactions. What is the BEST way to verify that the controls work as designed?

- ☒ Implement periodic reconciliations.
- ☐ Review quality assurance (QA) test results.
- ☐ Use generalized audit software for seeking data corresponding to duplicate transactions.
- ☐ Enter duplicate transactions in a copy of the live system.

Question 1842

Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

- ☐ Multiplexer
- ☒ Modem
- ☐ Protocol converter
- ☐ Concentrator

Explanation:

Explanation:

A modem is a device that translates data from digital to analog and back to digital.

Question 1843

An IS auditor performing an audit of backup procedures observes that backup tapes are picked up weekly and stored offsite at a third-party hosting facility. Which of the following recommendations would be the BEST way to protect the data on the backup tapes?

- ☒ Ensure that data is encrypted before leaving the facility.
- ☐ Ensure that the transport company obtains signatures for all shipments.
- ☐ Confirm that data is transported in locked tamper-evident containers.
- ☐ Confirm that data transfers are logged and recorded.

Question 1844

What should an IS auditor do if he or she observes that project-approval procedures do not exist?

- ☐ Advise senior management to invest in project-management training for the staff
- ☐ Create project-approval procedures for future project implementations
- ☐ Assign project leaders
- ☒ Recommend to management that formal approval procedures be adopted and documented

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and documented.

Question 1845

Within IPSEC which of the following defines security parameters which should be applied between communicating parties such as encryption algorithms, key initialization vector, life span of keys, etc?

- ☐ Security Parameter Index (SPI)
- ☒ Security Association (SA)
- ☐ Encapsulation Security Payload (ESP)
- ☐ Authentication Header (AH)

Explanation:

Security Association (SA)s defines which security parameters should be applied between communication parties as encryption algorithms, key initialization vector, life span of keys, etc.

For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.

In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and

Licensed to Berend Post berend.post@it-university.nl

attributes. For authentication, the sender uses digital certificates. The connection is made secure by supporting the generation, authentication, distribution of the SAs and the cryptographic keys.

The following were incorrect answers:

Security Parameter Index (SPI) – A Security Parameter Index (SPI) is an unique identifier that enables the sending host to reference the security parameters to apply.

Encapsulation Security Payload (ESP) – Encapsulation Security Payload (ESP) is used support authentication of sender and encryption of data.

Authentication Header(AH) – Authentication Header allows authentication of a sender of a data.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 353

Question 1846

The purpose of business continuity planning and disaster-recovery planning is to:

- ☐ Transfer the risk and impact of a business interruption or disaster
- ☒ Mitigate, or reduce, the risk and impact of a business interruption or disaster
- ☐ Accept the risk and impact of a business
- ☐ Eliminate the risk and impact of a business interruption or disaster

Explanation:

Explanation:

The primary purpose of business continuity planning and disaster-recovery planning is to mitigate, or reduce, the risk and impact of a business interruption or disaster.

Total elimination of risk is impossible.

Licensed to Berend Post berend.post@it-university.nl

Question 1847

A large insurance company is about to replace a major financial application. Which of the following is the IS auditor's PRIMARY focus when conducting the pre-implementation review?

- ☐ Procedure updates
- ☐ Migration of data
- ☐ System manuals
- ☒ Unit testing

Question 1848

A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

- ☐ Reviewing logs frequently
- ☒ Testing and validating the rules
- ☐ Training a local administrator at the new location
- ☐ Sharing firewall administrative duties

Explanation:

Explanation:

A mistake in the rule set can render a firewall insecure. Therefore, testing and validating the rules is the most important factor in ensuring a successful deployment. A regular review of log files would not start until the deployment has been completed. Training a local administrator may not be necessary if the firewalls are managed from a central location. Having multiple administrators is a good idea, but not the most important.

Question 1849

An IS auditor is reviewing the upgrading of an operating system. Which of the following would be the GREATEST audit concern?

- ☐ The lack of release notes
- ☒ The lack of change control
- ☐ The lack of malware protection
- ☐ The lack of activity logging

Licensed to Berend Post berend.post@it-university.nl

Question 1850

Following a successful attack on an organization's web server, which of the following actions should be performed FIRST?

- ☒ Review the boundary configuration rules to ensure that outbound packets are limited
- ☐ Evaluate and deploy an intrusion detection system
- ☐ Periodically scan the network for systems with well-known vulnerabilities
- ☐ Establish reference systems using cryptographic checksum tools

Question 1851

The PRIMARY objective of business continuity and disaster recovery plans should be to:

- ☐ safeguard critical IS assets.
- ☐ provide for continuity of operations.
- ☐ minimize the loss to an organization.
- ☒ protect human life.

Explanation:

Explanation:

Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

Question 1852

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- ☐ Issue an audit finding
- ☐ Seek an explanation from IS management
- ☐ Review the classifications of data held on the server
- ☒ Expand the sample of logs reviewed

Explanation:

Explanation:

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

Licensed to Berend Post berend.post@it-university.nl

Question 1853

Which of the following is the MOST likely result of the ongoing deterioration of a detective control?

- ☒ Increased number of data loss events
- ☐ Increased security incident response time
- ☐ Decreased effectiveness of root cause analysis
- ☐ Decreased overall recovery time

Question 1854

Which of the following is the MOST important outcome of effective risk treatment?

- ☐ Timely reporting of incidents
- ☐ Elimination of risk
- ☒ Implementation of corrective actions
- ☐ Reduced cost of maintaining controls

Question 1855

Which of the following is the MOST important consideration for an organization when strategizing to comply with privacy regulations?

- ☐ Ensuring there are staff members with in-depth knowledge of the privacy regulations
- ☐ Ensuring up-to-date knowledge of where customer data is saved
- ☐ Ensuring regularly updated contracts with third parties that process customer data
- ☒ Ensuring appropriate access to information systems containing privacy information.

Question 1856

The final decision to include a material finding in an audit report should be made by the:

- ☐ audit committee.
- ☐ auditee's manager.
- ☒ IS auditor.
- ☐ CEO of the organization

Explanation:

Explanation:

The IS auditor should make the final decision about what to include or exclude from the audit report. The other choices would limit the independence of the auditor.

Licensed to Berend Post berend.post@it-university.nl

Question 1857

Which of the following is MOST important for an IS auditor to determine when evaluating a database for privacy-related risks?

- ☐ Whether copies of production data are masked
- ☒ Whether the integrity of the data dictionary is maintained
- ☐ Whether data import and export procedures are approved
- ☐ Whether all database tables are normalized

Question 1858

The business case for an IS project has changed during the course of the project due to new requirements being added. What should be done NEXT?

- ☐ The project should go through the formal reapproval process.
- ☐ The changes to the business case should be documented in the project plan.
- ☐ Additional resources should be allocated to the project due to the new requirements.
- ☒ Project stakeholders should be notified of the changes.

Question 1859

Which of the following is MOSTimportant to consider when developing a bring your own device (BYOD) policy?

- ☐ Supported operating systems
- ☒ Procedure for accessing the network
- ☐ Application download restrictions
- ☐ Remote wipe procedures

Question 1860

When implementing a new risk assessment methodology, which of the following is the MOST important requirement?

- ☐ The methodology must be approved by the chief executive officer.
- ☐ Risk assessments must be reviewed annually.
- ☐ Risk assessments must be conducted by certified staff.
- ☒ The methodology used must be consistent across the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 1861

As described at security policy, the CSO implemented an e-mail package solution that allows for ensuring integrity of messages sent using SMIME. Which of the options below BEST describes how it implements the environment to suite policy's requirement?

- ☐ Implementing PGP and allowing for recipient to receive the private key used to sign e-mail message.
- ☒ Implementing RSA standard for messages envelope and instructing users to sign all messages using their private key from their PKI digital certificate.
- ☐ Implementing RSA standard for messages envelope and instructing users to sign all messages using their public key from their PKI digital certificate.
- ☐ Implementing MIME solutions and providing a footer within each message sent, referencing to policy constraints related to e-mail usage.

Explanation:

RSA e-mail standers stands for SMIME envelope. Using tm's private key to sign messages, users will ensure recipients of message integrity by using sender's public key for hash decryption and content comparison.

Exam candidates should be aware of e-mail solutions and technologies that addresses confidentiality, integrity and non-repudiation.

The following answers are incorrect:

Implementing PGP and allowing for recipient to receive the private key used to sign e-mail message.

Implementing RSA standard for messages envelope and instructing users to sign all messages using their public key from the PKI digital certificate.

Implementing MIME solutions and providing a footer within each message sent, referencing to policy constraints related to e-mail usage.

The following reference(s) were/was used to create this question:

CISA Review Manual 2010 - Chapter 5 - 5.4.5-Encryption - Digital Envelope

Licensed to Berend Post berend.post@it-university.nl

Question 1862

An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

- ☐ Nonavailability of an alternate private branch exchange (PBX) system
- ☒ Absence of a backup for the network backbone
- ☐ Lack of backup systems for the users' PCs
- ☐ Failure of the access card system

Explanation:

Explanation:

Failure of a network backbone will result in the failure of the complete network and impact the ability of all users to access information on the network. The nonavailability of an alternate PBX system will result in users not being able to make or receive telephone calls or faxes; however, users may have alternate means of communication, such as a mobile phone or e-mail. Lack of backup systems for user PCs will impact only the specific users, not all users. Failure of the access card system impacts the ability to maintain records of the users who are entering the specified work areas; however, this could be mitigated by manual monitoring controls.

Question 1863

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

- ☒ Substantive testing
- ☐ Walk-through reviews
- ☐ Compliance testing
- ☐ Design documentation reviews

Question 1864

The Federal Information Processing Standards (FIPS) are primarily for use by (Choose two.):

- ☒ all non-military government agencies
- ☒ US government contractors
- ☐ all military government agencies
- ☐ all private and public colleges in the US
- ☐ None of the choices.

Explanation:

Explanation:

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all nonmilitary government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community.

Licensed to Berend Post berend.post@it-university.nl

Question 1865

A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

- ☐ Rewrite the hard disk with random Os and Is.
- ☐ Low-level format the hard disk.
- ☐ Demagnetize the hard disk.
- ☒ Physically destroy the hard disk.

Explanation:

Explanation:

Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical, because the hard disk is damaged. Demagnetizing is an inefficient procedure, because it requires specialized and expensive equipment to be fully effective.

Question 1866

Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

- ☐ Reviewing program code
- ☒ Reviewing operations documentation
- ☐ Turning off the UPS, then the power
- ☐ Reviewing program documentation

Explanation:

Explanation:

Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

Question 1867

During an audit, which of the following would be MOST helpful in establishing a baseline for measuring data quality?

- ☐ Built-in data error prevention application controls
- ☐ Industry standard business definitions
- ☐ Input from customers
- ☒ Validation of rules by the business

Licensed to Berend Post berend.post@it-university.nl

Question 1868

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- ☐ Optimized
- ☒ Managed
- ☐ Defined
- ☐ Repeatable

Explanation:

Explanation:

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

Question 1869

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

Question 1870

Which is the PRIMARY objective of evaluating the readiness of information systems for implementation?

- ☐ Determine whether IT systems projects are on schedule.
- ☐ Determine whether the systems comply with the organization's policy.
- ☐ Determine whether the systems meet user requirements.
- ☒ Determine whether the systems meet business requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 1871

An IS auditor finds a number of system accounts that do not have documented approvals. Which of the following should be performed FIRST by the auditor?

- ☐ Have the accounts removed immediately
- ☐ Obtain sign-off on the accounts from the application owner
- ☐ Document a finding and report an ineffective account provisioning control
- ☒ Determine the purpose and risk of the accounts

Question 1872

During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

- ☒ review access control configuration
- ☐ evaluate interface testing.
- ☐ review detailed design documentation.
- ☐ evaluate system testing.

Explanation:

Explanation:

Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system. Since a postimplementation review is done after user acceptance testing and actual implementation, one would not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system, since these are usually vendor packages with user manuals. System testing should be performed before final user signoff.

Question 1873

Which of the following findings would have the GREATEST impact on the objective of a business intelligence system?

- ☐ Key control have not been tested in a year.
- ☐ Decision support queries use database functions proprietary to the vendor.
- ☐ The hot site for disaster recovery does not include the decision support system.
- ☒ Management reports have not been evaluated since implementation.

Licensed to Berend Post berend.post@it-university.nl

Question 1874

When performing an IS strategy audit, an IS auditor should review both short-term (one- year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

Question 1875

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

- ☐ has been approved by line management.
- ☐ does not vary from the IS department's preliminary budget.
- ☐ complies with procurement procedures.
- ☒ supports the business objectives of the organization.

Explanation:

Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrect since line management prepared the plans.

Question 1876

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan (DRP) has been successful?

- ☐ Evaluating participation by key personnel
- ☐ Testing at the backup data center
- ☒ Analyzing whether predetermined test objectives were met
- ☐ Testing with offsite backup files

Licensed to Berend Post berend.post@it-university.nl

Question 1877

A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ. Which of the following should be evaluated FIRST?

- ☒ Local regulatory requirements
- ☐ Local IT requirements
- ☐ Cross-border data mobility
- ☐ Corporate security objectives

Question 1878

Which of the following provides nonrepudiation in an electronic communication session without confidentiality?

- ☐ Message encryption
- ☐ Log-on ID and password
- ☐ Certification authority
- ☒ Digital signature

Question 1879

When using digital signatures, a sender transmits an encrypted message digest. This ensures that the:

- ☐ message is not intercepted during transmission
- ☒ message is not altered during transmission
- ☐ message sender obtains acknowledgement of delivery
- ☐ message remains confidential during transmission

Question 1880

What is a reliable technique for estimating the scope and cost of a software-development project?

- ☒ Function point analysis (FPA)
- ☐ Feature point analysis (FPA)
- ☐ GANTT
- ☐ PERT

Explanation:

Explanation:

A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

Licensed to Berend Post berend.post@it-university.nl

Question 1881

An IS auditor is performing a consulting engagement and needs to make a recommendation for securing all doors to a data center to prevent unauthorized access. Which of the following access control techniques would be MOST difficult for an intruder to compromise?

- ☐ Dead-man door and swipe card
- ☐ Smart card and numeric keypad
- ☐ USB token and password
- ☒ Biometrics and PIN

Question 1882

To develop a robust data security program, the FIRST course of action should be to:

- ☐ implement monitoring controls
- ☐ implement data loss prevention controls
- ☒ perform an inventory of assets
- ☐ interview IT senior management

Question 1883

An IS auditor notes that the anticipated benefits from an ongoing infrastructure project have changed due to recent organizational restructuring. Which of the following is the IS auditor's BEST recommendation?

- ☐ Review and reapprove the business case.
- ☒ Revise business goals and objectives.
- ☐ Conduct a new feasibility study.
- ☐ Review and update the business impact analysis (BIA).

Question 1884

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

- ☒ symmetric encryption.
- ☐ message authentication code.
- ☐ hash function.
- ☐ digital signature certificates.

Explanation:

Explanation:

SSL uses a symmetric key for message encryption. A message authentication code is used for ensuring data integrity. Hash function is used for generating a message digest; it does not use public key encryption for message encryption. Digital signature certificates are used by SSL for server authentication.

Licensed to Berend Post berend.post@it-university.nl

Question 1885

On a public-key cryptosystem when there is no previous knowledge between parties, which of the following will BEST help to prevent one person from using a fictitious key to impersonate someone else?

- ☐ Encrypt the message containing the sender's public key, using a private-key cryptosystem.
- ☒ Send a certificate that can be verified by a certification authority with the public key.
- ☐ Encrypt the message containing the sender's public key; using the recipient's pubic key.
- ☐ Send the public key to the recipient prior to establishing the connection.

Question 1886

An IS auditor considering use of another auditor's workpapers should:

- ☐ rarely rely on the work of another auditor.
- ☐ determine that the workpapers were completed within the past month.
- ☒ determine that then auditee agrees with key issues in these workpapers.
- ☐ consider the appropriateness and sufficiency of the workpapers.

Question 1887

After observing suspicious activities in a server, a manager requests a forensic analysis.
Which of the following findings should be of MOST concern to the investigator?

- ☐ Server is a member of a workgroup and not part of the server domain
- ☐ Guest account is enabled on the server
- ☐ Recently, 100 users were created in the server
- ☒ Audit logs are not enabled for the server

Explanation:

Explanation:

Audit logs can provide evidence which is required to proceed with an investigation and should not be disabled. For business needs, a server can be a member of a workgroup and, therefore, not a concern. Having a guest account enabled on a system is a poor security practice but not a forensic investigation concern. Recently creating 100 users in the server may have been required to meet business needs and should not be a concern.

Licensed to Berend Post berend.post@it-university.nl

Question 1888

An IS auditor reviews an organizational chart PRIMARILY for:

- ☐ an understanding of workflows.
- ☐ investigating various communication channels.
- ☒ understanding the responsibilities and authority of individuals.
- ☐ investigating the network connected to different employees.

Explanation:

Explanation: An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

Question 1889

During audit follow-up, an IS auditor finds that a control has been implemented differently than recommended. The auditor should:

- ☐ verify whether the control objectives are adequately addressed.
- ☒ compare the control to the action plan.
- ☐ report as a repeat finding.
- ☐ inform management about incorrect implementation.

Question 1890

Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

- ☐ Circuit gateway
- ☒ Application gateway
- ☐ Packet filter
- ☐ Screening router

Explanation:

Explanation:

An application gateway firewall is effective in preventing applications, such as FTPs, from entering the organization network. A circuit gateway firewall is able to prevent paths or circuits, not applications, from entering the organization's network. A packet filter firewall or screening router will allow or prevent access based on IP packets/address.

Licensed to Berend Post berend.post@it-university.nl

Question 1891

Which of the following is the BEST source of information for an IS auditor when planning an audit of a business application's controls?

- ☒ User documentation
- ☐ Change control procedures
- ☐ Access control lists
- ☐ Process flow diagrams

Question 1892

Which of the following will BEST provide an organization with ongoing assurance of the information security services provided by a cloud provider?

- ☒ Continuous monitoring of an information security risk profile
- ☐ Evaluating the provider's security incident response plan
- ☐ Requiring periodic self-assessment by the provider
- ☐ Ensuring the provider's roles and responsibilities are established

Question 1893

An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

- ☐ reverse engineering.
- ☐ prototyping.
- ☐ software reuse.
- ☒ reengineering.

Explanation:

Explanation:

Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

Licensed to Berend Post berend.post@it-university.nl

Question 1894

Which of the following are BEST suited for continuous auditing?

- ☐ Manual transactions
- ☐ Irregular transactions
- ☐ Low-value transactions
- ☒ Real-time transactions

Question 1895

Which of the following acts as a decoy to detect active internet attacks?

- ☒ Honeypots
- ☐ Firewalls
- ☐ Trapdoors
- ☐ Traffic analysis

Explanation:

Explanation:

Honeypots are computer systems that are expressly set up to attract and trap individuals who attempt to penetrate other individuals' computer systems. The concept of a honeypot is to learn from intruder's actions. A properly designed and configured honeypot provides data on methods used to attack systems. The data are then used to improve measures that could curb future attacks. A firewall is basically a preventive measure. Trapdoors create a vulnerability that provides an opportunity for the insertion of unauthorized code into a system. Traffic analysis is a type of passive attack.

Question 1896

What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

- ☐ A star network topology
- ☒ A mesh network topology with packet forwarding enabled at each host
- ☐ A bus network topology
- ☐ A ring network topology

Explanation:

Explanation:

A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance.

Licensed to Berend Post berend.post@it-university.nl

Question 1897

The BEST overall quantitative measure of the performance of biometric control devices is:

- ☐ false-rejection rate.
- ☐ false-acceptance rate.
- ☒ equal-error rate.
- ☐ estimated-error rate.

Explanation:

Explanation:

A low equal-error rate (EER) is a combination of a low false-rejection rate and a low false- acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false-rejection and false-acceptance rates are equal. A low EER is the measure of the more effective biometrics control device. Low false-rejection rates or low false- acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is nonexistent and therefore irrelevant.

Question 1898

Which of the following would be an IS auditor's GREATEST concern when evaluating a cybersecurity incident response plan?

- ☐ The plan has not been recently tested.
- ☒ Roles and responsibilities are not detailed for each process.
- ☐ Stakeholder contact details are not up-to-date.
- ☐ The plan does not include incident response metrics.

Question 1899

Which of the following must be in place before an IS auditor initiates audit follow-up activities?

- ☐ A heat map with the gaps and recommendations displayed in terms of risk
- ☐ A management response in the final report with a committed implementation date
- ☒ Supporting evidence for the gaps and recommendations mentioned in the audit report
- ☐ Available resources for the activities included in the action plan

Question 1900

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- ☒ understand the business process.
- ☐ comply with auditing standards.
- ☐ identify control weakness.
- ☐ plan substantive testing.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

Question 1901

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

- ☐ Palm Scan
- ☐ Hand Geometry
- ☐ Fingerprint
- ☒ Retina scan

Explanation:

Retina based biometric involves analyzing the layer of blood vessels situated at the back of the eye.

An established technology, this technique involves using a low-intensity light source through an optical coupler to scan the unique patterns of the retina. Retinal scanning can be quite accurate but does require the user to look into a receptacle and focus on a given point. This is not particularly convenient if you wear glasses or are concerned about having close contact with the reading device. For these reasons, retinal scanning is not warmly accepted by all users, even though the technology itself can work well.

For your exam you should know the information below:

Biometrics

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of verifying identification and not well received by society. Biometrics is a very sophisticated technology; thus, it is much more expensive and complex than the other types of identity verification processes. A biometric system can make authentication decisions based on an individual's behavior, as in signature dynamics, but these can change over time and possibly be forged. Biometric systems that base authentication decisions on physical attributes (such as iris, retina, or fingerprint) provide more accuracy because physical attributes typically don't change, absent some disfiguring injury, and are harder to impersonate

Biometrics is typically broken up into two different categories. The first is the physiological. These are traits that are physical attributes unique to a specific individual. Fingerprints are a common example of a physiological trait used in biometric systems. The second category of biometrics is known as behavioral. The behavioral authentication is also known as continuous authentication. The behavioral/continuous authentication prevents session hijacking attack. This is based on a

Licensed to Berend Post berend.post@it-university.nl

characteristic of an individual to confirm his identity. An example is signature Dynamics. Physiological is “what you are” and behavioral is “what you do.”

When a biometric system rejects an authorized individual, it is called a Type I error (false rejection rate). When the system accepts impostors who should be rejected, it is called a Type II error (false acceptance rate). The goal is to obtain low numbers for each type of error, but Type II errors are the most dangerous and thus the most important to avoid.

When comparing different biometric systems, many different variables are used, but one of the most important metrics is the crossover error rate (CER). This rating is stated as a percentage and represents the point at which the false rejection rate equals the false acceptance rate. This rating is the most important measurement when determining the system’s accuracy. A biometric system that delivers a CER of 3 will be more accurate than a system that delivers a CER of 4. Crossover error rate (CER) is also called equal error rate (EER).

Throughput describes the process of authenticating to a biometric system. This is also referred to as the biometric system response time. The primary consideration that should be put into the purchasing and implementation of biometric access control are user acceptance, accuracy and processing speed.

Biometric Considerations

In addition to the access control elements of a biometric system, there are several other considerations that are important to the integrity of the control environment. These are:

Resistance to counterfeiting

Data storage requirements

User acceptance

Reliability and

Target User and approach

Fingerprint

Fingerprints are made up of ridge endings and bifurcations exhibited by friction ridges and other detailed characteristics called minutiae. It is the distinctiveness of these minutiae that gives each individual a unique fingerprint. An individual places his finger on a device that reads the details of the fingerprint and compares this to a reference file. If the two match, the individual’s identity has been verified.

Palm Scan

Licensed to Berend Post berend.post@it-university.nl

The palm holds a wealth of information and has many aspects that are used to identify an individual. The palm has creases, ridges, and grooves throughout that are unique to a specific person. The palm scan also includes the fingerprints of each finger. An individual places his hand on the biometric device, which scans and captures this information. This information is compared to a reference file, and the identity is either verified or rejected.

Hand Geometry

The shape of a person's hand (the shape, length, and width of the hand and fingers) defines hand geometry. This trait differs significantly between people and is used in some biometric systems to verify identity. A person places her hand on a device that has grooves for each finger. The system compares the geometry of each finger, and the hand as a whole, to the information in a reference file to verify that person's identity.

Retina Scan

A system that reads a person's retina scans the blood-vessel pattern of the retina on the backside of the eyeball. This pattern has shown to be extremely unique between different people. A camera is used to project a beam inside the eye and capture the pattern and compare it to a reference file recorded previously.

Iris Scan

An iris scan is a passive biometric control

The iris is the colored portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colors, rings, coronas, and furrows. The uniqueness of each of these characteristics within the iris is captured by a camera and compared with the information gathered during the enrollment phase.

When using an iris pattern biometric system, the optical unit must be positioned so the sun does not shine into the aperture; thus, when implemented, it must have proper placement within the facility.

Signature Dynamics

When a person signs a signature, usually they do so in the same manner and speed each time. Signing a signature produces electrical signals that can be captured by a biometric system. The physical motions performed when someone is signing a document create these electrical signals. The signals provide unique characteristics that can be used to distinguish one individual from another. Signature dynamics provides more information than a static signature, so there are more variables to verify when confirming an individual's identity and more assurance that this person is who he claims to be.

Keystroke Dynamics

Whereas signature dynamics is a method that captures the electrical signals when a person signs a name, keystroke dynamics captures electrical signals when a person types a certain phrase. As a

Licensed to Berend Post berend.post@it-university.nl

person types a specified phrase, the biometric system captures the speed and motions of this action. Each individual has a certain style and speed, which translate into unique signals. This type of authentication is more effective than typing in a password, because a password is easily obtainable. It is much harder to repeat a person's typing style than it is to acquire a password.

Voice Print

People's speech sounds and patterns have many subtle distinguishing differences. A biometric system that is programmed to capture a voice print and compare it to the information held in a reference file can differentiate one individual from another. During the enrollment process, an individual is asked to say several different words.

Facial Scan

A system that scans a person's face takes many attributes and characteristics into account. People have different bone structures, nose ridges, eye widths, forehead sizes, and chin shapes. These are all captured during a facial scan and compared to an earlier captured scan held within a reference record. If the information is a match, the person is positively identified.

Hand Topography

Whereas hand geometry looks at the size and width of an individual's hand and fingers, hand topology looks at the different peaks and valleys of the hand, along with its overall shape and curvature. When an individual wants to be authenticated, she places her hand on the system. Off to one side of the system, a camera snaps a side-view picture of the hand from a different view and angle than that of systems that target hand geometry, and thus captures different data. This attribute is not unique enough to authenticate individuals by itself and is commonly used in conjunction with hand geometry.

Vascular Scan

Vascular Scan uses the blood vessel under the first layer of skin.

The following answers are incorrect:

Fingerprint - Fingerprints are made up of ridge endings and bifurcations exhibited by friction ridges and other detailed characteristics called minutiae. It is the distinctiveness of these minutiae that gives each individual a unique fingerprint. An individual places his finger on a device that reads the details of the fingerprint and compares this to a reference file. If the two match, the individual's identity has been verified.

Licensed to Berend Post berend.post@it-university.nl

Hand Geometry - The shape of a person's hand (the shape, length, and width of the hand and fingers) defines hand geometry. This trait differs significantly between people and is used in some biometric systems to verify identity. A person places her hand on a device that has grooves for each finger. The system compares the geometry of each finger, and the hand as a whole, to the information in a reference file to verify that person's identity.

Palm Scan - The palm holds a wealth of information and has many aspects that are used to identify an individual. The palm has creases, ridges, and grooves throughout that are unique to a specific person. The palm scan also includes the fingerprints of each finger. An individual places his hand on the biometric device, which scans and captures this information. This information is compared to a reference file, and the identity is either verified or rejected.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 330 and 331

Official ISC2 guide to CISSP CBK 3rd Edition Page number 924

Question 1902

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- ☐ Governing
- ☐ Culture
- ☐ Enabling and support
- ☒ Emergence

Explanation:

Explanation:

Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

For your exam you should know the information below.

Business Model for Information Security

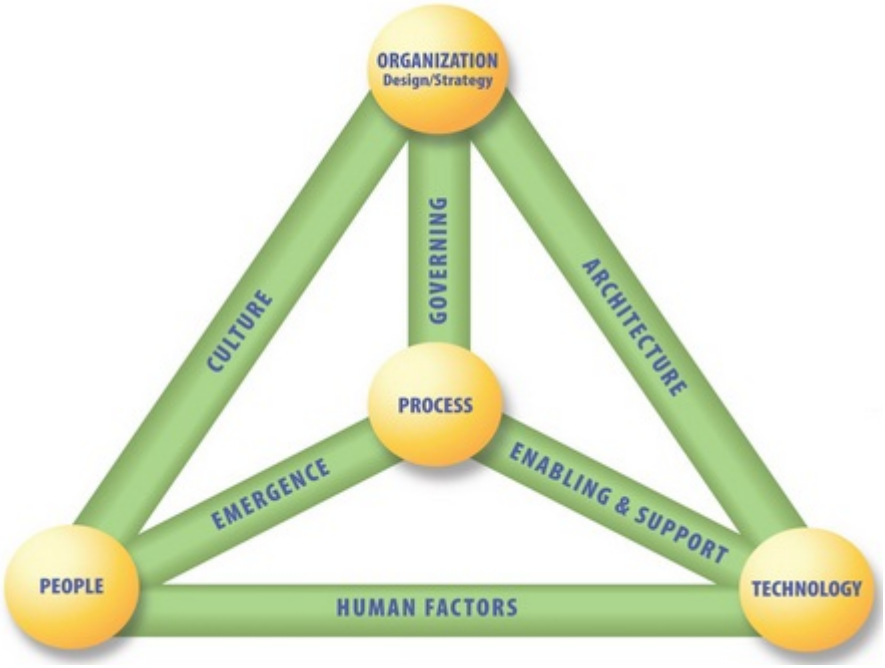
Licensed to Berend Post berend.post@it-university.nl

The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. "Systems thinking" is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why "the whole is more than the sum of its parts." Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.

Licensed to Berend Post berend.post@it-university.nl



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.

All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

1. Organization Design and Strategy—An organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People—The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:

Licensed to Berend Post berend.post@it-university.nl

Recruitment strategies (access, background checks, interviews, roles and responsibilities)

Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)

Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process—Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.

Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology—Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

Licensed to Berend Post berend.post@it-university.nl

1. Governing—Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

2. Culture—Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support—The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence—Emergence—which connotes surfacing, developing, growing and evolving—refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

5. Human factors—The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.

Licensed to Berend Post berend.post@it-university.nl

6. Architecture—A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Culture - Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 37 and 38

http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

Licensed to Berend Post berend.post@it-university.nl

Question 1903

Which of the following is a network diagnostic tool that monitors and records network information?

- ☐ Online monitor
- ☐ Downtime report
- ☐ Help desk report
- ☒ Protocol analyzer

Explanation:

Explanation:

Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

Question 1904

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

- ☒ Blackbox test
- ☐ Desk checking
- ☐ Structured walk-through
- ☐ Design and code

Explanation:

Explanation:

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules, a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

Question 1905

What is an edit check to determine whether a field contains valid data?

- ☒ Completeness check
- ☐ Accuracy check
- ☐ Redundancy check
- ☐ Reasonableness check

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A completeness check is an edit check to determine whether a field contains valid data.

Question 1906

An organization is in the process of acquiring a competitor. The information security manager has been asked to report on the security posture of the target acquisition. Which of the following should be the security manager's FIRSTcourse of action?

- ☒ Implement a security dashboard
- ☐ Quantity the potential risk
- ☐ Perform a gap analysis
- ☐ Perform a vulnerability assessment

Question 1907

Which of the following BEST describes the concept of ""defense in depth""?

- ☒ more than one subsystem needs to be compromised to compromise the security of the system and the information it holds.
- ☐ multiple firewalls are implemented.
- ☐ multiple firewalls and multiple network OS are implemented.
- ☐ intrusion detection and firewall filtering are required.
- ☐ None of the choices.

Explanation:

Explanation:

"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure""."

Question 1908

A potential risk of executing a program on an Internet site is that it may:

- ☒ install executable code on the computer.
- ☐ lack version control, which may result in the use of an older program.
- ☐ overwrite system files with older versions.
- ☐ be browser-dependent, and therefore abort.

Licensed to Berend Post berend.post@it-university.nl

Question 1909

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

- ☐ schedule the audits and monitor the time spent on each audit.
- ☐ train the IS audit staff on current technology used in the company.
- ☒ develop the audit plan on the basis of a detailed risk assessment.
- ☐ monitor progress of audits and initiate cost control measures.

Explanation:

Explanation:

Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

Question 1910

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

Question 1911

When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:

- ☐ carry the flash drive in a portable safe.
- ☐ assure management that you will not lose the flash drive.
- ☐ request that management deliver the flash drive by courier.
- ☒ encrypt the folder containing the data with a strong key.

Explanation:

Explanation:

Encryption, with a strong key, is the most secure method for protecting the information on the flash drive. Carrying the flash drive in a portable safe does not guarantee the safety of the information in the event that the safe is stolen or lost. No matter what measures you take, the chance of losing the flash drive still exists. It is possible that a courier might lose the flash drive or that it might be stolen.

Licensed to Berend Post berend.post@it-university.nl

Question 1912

Which of the following is the MOST effective control in an organization to mitigate the risk of insider misuse of personal devices?

- ☐ Security risk assessments
- ☐ Periodic vulnerability scanning
- ☐ Security awareness training
- ☒ Comprehensive procedures on data security

Question 1913

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- ☐ address all of the network risks.
- ☐ be tracked over time against the IT strategic plan.
- ☒ take into account the entire IT environment.
- ☐ result in the identification of vulnerability tolerances.

Explanation:

Explanation:

When assessing IT security risk, it is important to take into account the entire IT environment. Measures of security risk should focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost. IT strategic plans are not granular enough to provide appropriate measures. Objective metrics must be tracked over time against measurable goals, thus the management of risk is enhanced by comparing today's results against last week, last month, last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk. They do not identify tolerances.

Question 1914

Which of the following provides the BEST indication that the information security program is in alignment with enterprise requirements?

- ☐ The security strategy is benchmarked with similar organizations.
- ☐ The information security manager reports to the chief executive officer.
- ☐ An IT governance committee is in place.
- ☒ Security strategy objectives are defined in business terms.

Licensed to Berend Post berend.post@it-university.nl

Question 1915

After an IS auditor has identified threats and potential impacts, the auditor should:

- ☒ Identify and evaluate the existing controls
- ☐ Conduct a business impact analysis (BIA)
- ☐ Report on existing controls
- ☐ Propose new controls

Explanation:

Explanation:

After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls.

Question 1916

An accounting department uses a spreadsheet to calculate sensitive financial transactions. Which of the following is the MOST important control for maintaining the security of data in the spreadsheet?

- ☒ There is a reconciliation process between the spreadsheet and the finance system.
- ☐ The spreadsheet is locked down to avoid inadvertent changes.
- ☐ A separate copy of the spreadsheet is routinely backed up.
- ☐ Access to the spreadsheet is given only to those who require access.

Question 1917

Which of the following controls would BEST detect intrusion?

- ☐ User IDs and user privileges are granted through authorized procedures.
- ☐ Automatic logoff is used when a workstation is inactive for a particular period of time.
- ☐ Automatic logoff of the system occurs after a specified number of unsuccessful attempts.
- ☒ Unsuccessful logon attempts are monitored by the security administrator.

Explanation:

Explanation:

Intrusion is detected by the active monitoring and review of unsuccessful logons. User IDs and the granting of user privileges define a policy, not a control. Automatic logoff is a method of preventing access on inactive terminals and is not a detective control. Unsuccessful attempts to log on are a method for preventing intrusion, not detecting.

Licensed to Berend Post berend.post@it-university.nl

Question 1918

Host Based ILD&P primarily addresses the issue of:

- ☐ information integrity
- ☐ information accuracy
- ☐ information validity
- ☒ information leakage
- ☐ None of the choices.

Explanation:

Explanation:

Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

Question 1919

What is the MOST important role of an organization's data custodian in support of information security function?

- ☐ Evaluating data security technology vendors
- ☐ Applying approval security policies
- ☒ Approving access rights to departmental data
- ☐ Assessing data security risks to the organization

Question 1920

When planning an audit to assess application controls of a cloud-based system, it is MOST important for the IS auditor to understand the:

- ☒ policies and procedures of the business area being audited.
- ☐ business process supported by the system.
- ☐ availability reports associated with the cloud-based system.
- ☐ architecture and cloud environment of the system.

Licensed to Berend Post berend.post@it-university.nl

Question 1921

The BEST method an organization can employ to align its business continuity plan (BCP) and disaster recovery plan (DRP) with core business needs is to:

- ☐ execute periodic walk-throughs of the plans.
- ☒ update the business impact analysis (BIA) for significant business changes.
- ☐ outsource the maintenance of the BCP and disaster recovery plan to a third party.
- ☐ include BCP and disaster recovery plan responsibilities as a part of new employee training.

Question 1922

When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

- ☐ systems receiving the output of other systems.
- ☐ systems sending output to other systems.
- ☒ systems sending and receiving data.
- ☐ interfaces between the two systems.

Explanation:

Explanation:

Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

Question 1923

Which of the following layer of an OSI model encapsulates packets into frames?

- ☐ Transport Layer
- ☐ Network Layer
- ☒ Data Link Layer
- ☐ Physical Layer
- ☐ .

Explanation:

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

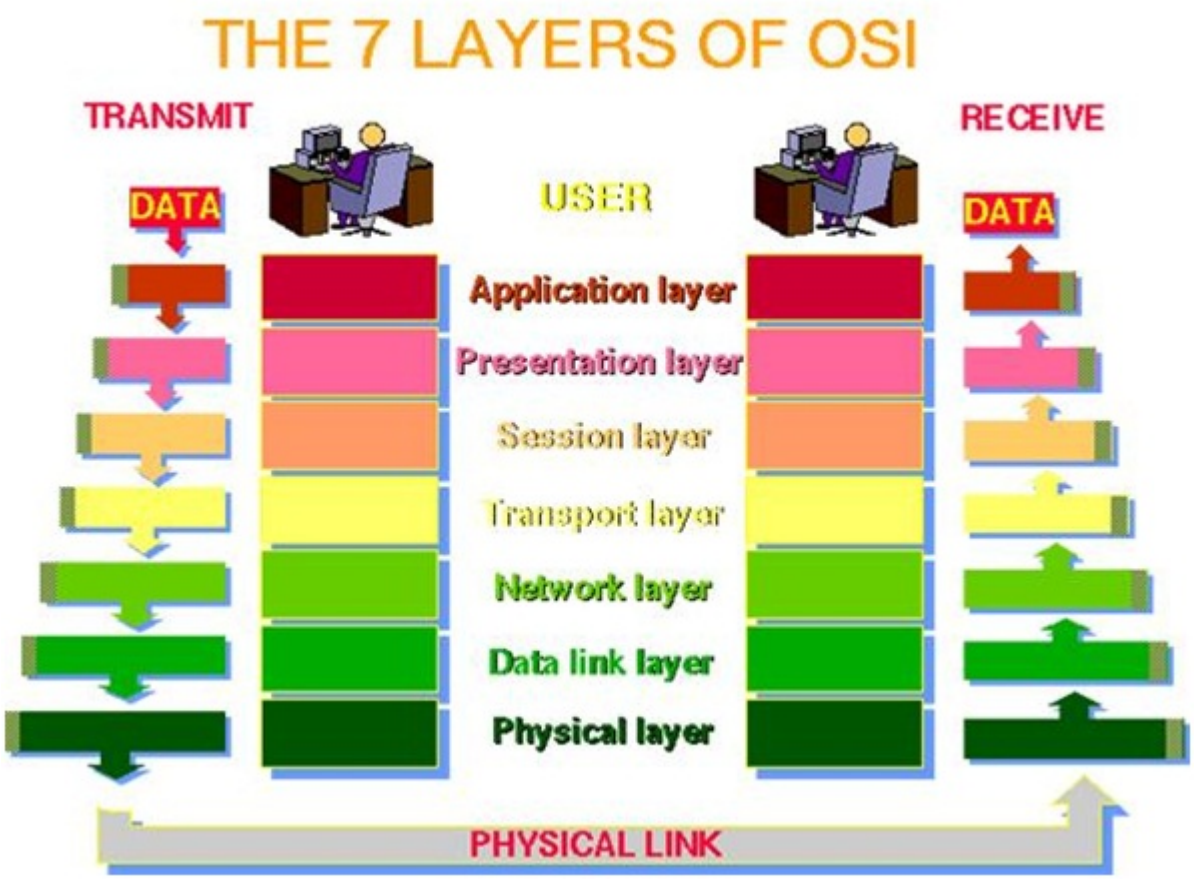
For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

Licensed to Berend Post berend.post@it-university.nl

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

Licensed to Berend Post berend.post@it-university.nl

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

Licensed to Berend Post berend.post@it-university.nl

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

Licensed to Berend Post berend.post@it-university.nl

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Licensed to Berend Post berend.post@it-university.nl

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.

Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Question 1924

While reviewing similar issues in an organization's help desk system, an IS auditor finds that they were analyzed independently and resolved differently. This situation MOST likely indicates a deficiency in:

- ☐ IT service level management.
- ☐ change management.
- ☐ configuration management.
- ☒ problem management.

Licensed to Berend Post berend.post@it-university.nl

Question 1925

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

- ☐ Automated electronic journaling and parallel processing
- ☒ Data mirroring and parallel processing
- ☐ Data mirroring
- ☐ Parallel processing

Explanation:

Explanation:

Data mirroring and parallel processing are both used to provide near- immediate recoverability for time-sensitive systems and transaction processing.

Question 1926

The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

- ☐ compression software to minimize transmission duration.
- ☐ functional or message acknowledgments.
- ☐ a packet-filtering firewall to reroute messages.
- ☒ leased asynchronous transfer mode lines.

Explanation:

Explanation:

Leased asynchronous transfer mode lines are a way to avoid using public and shared infrastructures from the carrier or Internet service provider that have a greater number of communication failures. Choice A, compression software, is a valid way to reduce the problem, but is not as good as leased asynchronous transfer mode lines. Choice B is a control based on higher protocol layers and helps if communication lines are introducing noise, but not if a link is down. Choice C, a packet-filtering firewall, does not reroute messages.

Question 1927

To ensure efficient and economic use of limited resources in supporting a local area network (LAN) infrastructure, it is advisable to:

- ☐ periodically rotate vendors to obtain the best price-to-performance ratio.
- ☒ standardize on a limited number of device models and software applications.
- ☐ quickly upgrade to the latest hardware and software versions to take advantage of new features.
- ☐ recommend a variety of products so that user effectiveness and flexibility can be maximized.

Licensed to Berend Post berend.post@it-university.nl

Question 1928

Which of the following is the MOST effective way of ensuring that business units comply with an information security governance framework?

- ☐ Conducting information security awareness training
- ☐ Performing security assessments and gap analyses
- ☒ Integrating security requirements with processes
- ☐ Conducting a business impact analysis (BIA)

Question 1929

An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor's NEXT course of action?

- ☐ Determine the value of the firewall.
- ☐ Report the security posture of the organization.
- ☐ Report the mitigating controls.
- ☒ Determine the risk of not replacing the firewall.

Question 1930

Which of the following is the MOST appropriate document for granting authority to an external IS auditor in an audit engagement with a client organization?

- ☒ Approved statement of work
- ☐ Formally approved audit charter
- ☐ An internal memo to all concerned parties
- ☐ Request for proposal for audit services

Question 1931

An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?

- ☐ Requiring policy acknowledgment and nondisclosure agreements signed by employees
- ☒ Providing education and guidelines to employees on use of social networking sites
- ☐ Establishing strong access controls on confidential data
- ☐ Monitoring employees' social networking usage

Licensed to Berend Post berend.post@it-university.nl

Question 1932

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

- ☐ A substantive test of program library controls
- ☒ A compliance test of program library controls
- ☐ A compliance test of the program compiler controls
- ☐ A substantive test of the program compiler controls

Explanation:

Explanation:

A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

Question 1933

Security administration procedures require read-only access to:

- ☐ access control tables.
- ☒ security log files.
- ☐ logging options.
- ☐ user profiles.

Explanation:

Explanation:

Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and user activities are monitored, captured, stored, processed and reported.

Question 1934

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

- ☒ True
- ☐ False

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

Question 1935

When physical destruction is not practical, which of the following is the MOST effective means of disposing of sensitive data on a hard disk?

- ☐ Recycling the disk
- ☐ Reformatting
- ☐ Deleting files sequentially
- ☒ Overwriting multiple times

Question 1936

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions.

Question 1937

What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management?

- ☐ The software can dynamically readjust network traffic capabilities based upon current usage.
- ☐ The software produces nice reports that really impress management.
- ☐ It allows users to properly allocate resources and ensure continuous efficiency of operations.
- ☒ It allows management to properly allocate resources and ensure continuous efficiency of operations.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

Question 1938

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain an effective information security program?

- ☒ Determine new factors that could influence the information security strategy.
- ☐ Implement the current information security program in the acquired company.
- ☐ Merge the two information security programs to establish continuity.
- ☐ Ensure information security is included in any change control efforts.

Question 1939

Which of the following type of a computer network are variation of LAN and are dedicated to connecting storage devices to servers and other computing devices?

- ☐ LAN
- ☐ MAN
- ☒ SAN
- ☐ PAN

Explanation:

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

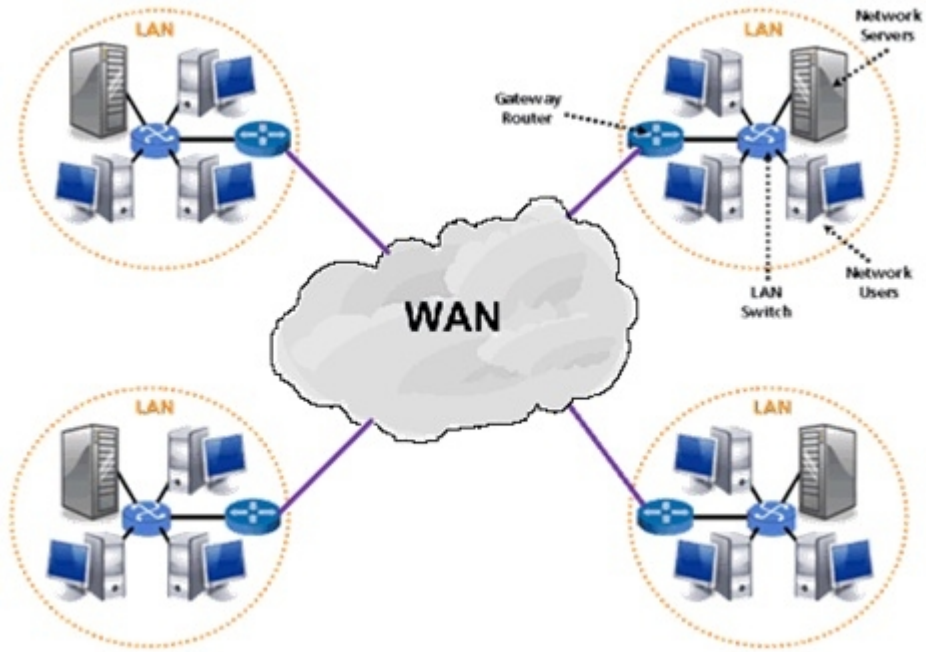
Local Area Network

Licensed to Berend Post berend.post@it-university.nl

Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Wide Area Network

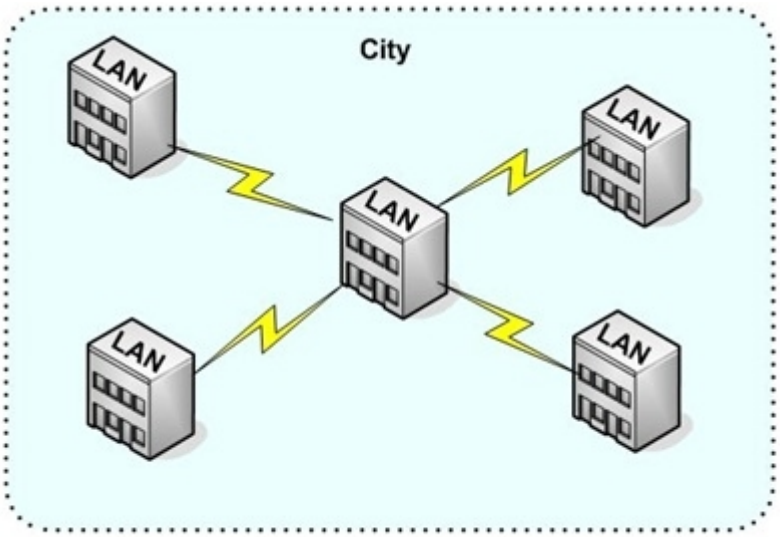


Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

Licensed to Berend Post berend.post@it-university.nl

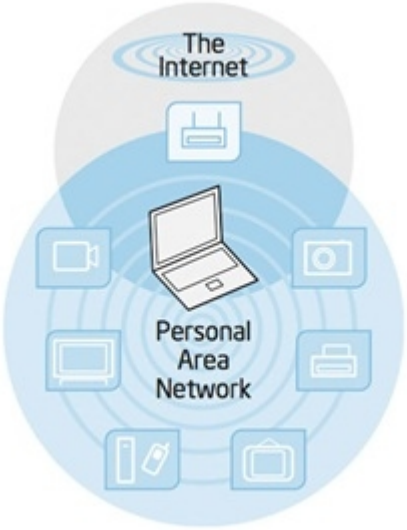


Metropolitan Area Network (MAN)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to

Licensed to Berend Post berend.post@it-university.nl

the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

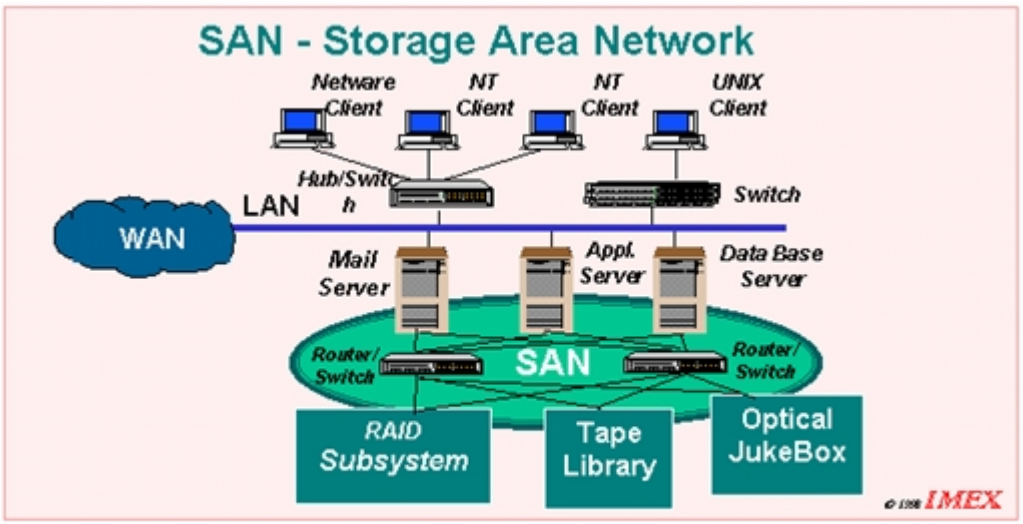


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Licensed to Berend Post berend.post@it-university.nl

Question 1940

When reviewing a disaster recovery plan (DRP), an IS auditor should examine the:

- ☒ access to the computer site by backup staff.
- ☐ offsite data file storage.
- ☐ uninterruptible power supply (UPS).
- ☐ fire-fighting equipment.

Question 1941

Which of the following type of an IDS resides on important systems like database, critical servers and monitors various internal resources of an operating system?

- ☐ Signature based IDS
- ☒ Host based IDS
- ☐ Network based IDS
- ☐ Statistical based IDS

Explanation:

Host Based IDS resides on important systems like database, critical servers and monitors various internal resources of an operating system.

Also, you should know below mentioned categories and types of IDS for CISA exam

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies.

Broad categories of IDS include:

1. Network Based IDS

2. Host Based IDS

Network Based IDS

They identify attack within the monitored network and issue a warning to the operator.

If a network based IDS is placed between the Internet and the firewall, it will detect all the attack attempts whether or not they enter the firewall

Network Based IDS are blinded when dealing with encrypted traffic

Licensed to Berend Post berend.post@it-university.nl

Host Based IDS

They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack.

They can detect the modification of executable programs, detect the detection of files and issue a warning when an attempt is made to use a privilege account.

They can monitor traffic after it is decrypted and they supplement the Network Based IDS.

Types of IDS includes:

Statistical Based IDS – This system needs a comprehensive definition of the known and expected behavior of system

Neural Network – An IDS with this feature monitors the general patterns of activity and traffic on the network, and create a database. This is similar to statistical model but with added self-learning functionality.

Signature Based IDS – These IDS system protect against detected intrusion patterns. The intrusive pattern they can identify are stored in the form of signature.

The following were incorrect answers:

The other types of IDS mentioned in the options do not resides on important systems like database and critical servers

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 346 and 347

Licensed to Berend Post berend.post@it-university.nl

Question 1942

Which of the following is the GREATEST concern when an organization's backup facility is at a warm site?

- ☒ Timely availability of hardware
- ☐ Availability of heat, humidity and air conditioning equipment
- ☐ Adequacy of electrical power connections
- ☐ Effectiveness of the telecommunications network

Explanation:

Explanation:

A warm site has the basic infrastructure facilities implemented, such as power, air conditioning and networking, but is normally lacking computing equipment. Therefore, the availability of hardware becomes a primary concern.

Question 1943

Which of the following is the BEST practice to ensure that access authorizations are still valid?

- ☐ information owner provides authorization for users to gain access
- ☒ identity management is integrated with human resource processes
- ☐ information owners periodically review the access controls
- ☐ An authorization matrix is used to establish validity of access

Explanation:

Explanation:

Personnel and departmental changes can result in authorization creep and can impact the effectiveness of access controls. Many times when personnel leave an organization, or employees are promoted, transferred or demoted, their system access is not fully removed, which increases the risk of unauthorized access. The best practices for ensuring access authorization is still valid is to integrate identity management with human resources processes. When an employee transfers to a different function, access rights are adjusted at the same time.

Question 1944

What is/are used to measure and ensure proper network capacity management and availability of services?

- ☒ Network performance-monitoring tools
- ☐ Network component redundancy
- ☐ Syslog reporting
- ☐ IT strategic planning

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

Question 1945

Which of the following is the GREATEST risk resulting from conducting periodic reviews of IT over several years based on the same audit program?

- ☐ The amount of errors will increase because the routine work promotes inattentiveness.
- ☐ Detection risk is increased because auditees already know the audit program.
- ☒ Audit risk is increased because the programs might not be adapted to the organization's current situation.
- ☐ Staff turnover in the audit department will increase because fieldwork becomes less interesting.

Question 1946

Which of the following is the GREATEST benefit of implementing an incident management process?

- ☐ Opportunity for frequent reassessment of incidents
- ☐ Reduction in security threats
- ☒ Reduction in the business impact of incidents
- ☐ Reduction of costs by the efficient use of resources

Question 1947

Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

- ☐ A remote access server
- ☐ A proxy server
- ☒ A personal firewall
- ☐ A password-generating token

Explanation:

Explanation:

A personal firewall is the best way to protect against hacking, because it can be defined with rules that describe the type of user or connection that is or is not permitted. A remote access server can be mapped or scanned from the Internet, creating security exposures. Proxy servers can provide protection based on the IP address and ports; however, an individual would need to have in-depth knowledge to do this, and applications can use different ports for the different sections of their program. A password-generating token may help to encrypt the session but does not protect a computer against hacking.

Licensed to Berend Post berend.post@it-university.nl

Question 1948

Which of the following potentially blocks hacking attempts?

- ☐ intrusion detection system
- ☐ Honeypot system
- ☒ Intrusion prevention system
- ☐ Network security scanner

Explanation:

Explanation:

An intrusion prevention system (IPS) is deployed as an in-line device that can detect and block hacking attempts. An intrusion detection system (IDS) normally is deployed in sniffing mode and can detect intrusion attempts, but cannot effectively stop them. A honeypot solution traps the intruders to explore a simulated target. A network security scanner scans for the vulnerabilities, but it will not stop the intrusion.

Question 1949

Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems?

- ☐ An increase in the number of identified false positives
- ☐ An increase in the number of unfamiliar sources of intruders
- ☒ An increase in the number of detected incidents not previously identified
- ☐ An increase in the number of internally reported critical incidents

Question 1950

Which of the following would be an INAPPROPRIATE activity for a network administrator?

- ☐ Analyzing network security incidents
- ☐ Prioritizing traffic between subnets
- ☐ Modifying a router configuration
- ☒ Modifying router log files

Question 1951

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

- ☐ whose sum of activity time is the shortest.
- ☒ that have zero slack time.
- ☐ that give the longest possible completion time.
- ☐ whose sum of slack time is the shortest.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities on the critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

Question 1952

Whenever an application is modified, what should be tested to determine the full impact of the change?

- ☐ Interface systems with other applications or systems
- ☒ The entire program, including any interface systems with other applications or systems
- ☐ All programs, including interface systems with other applications or systems
- ☐ Mission-critical functions and any interface systems with other applications or systems

Explanation:

Explanation:

Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

Question 1953

Involvement of senior management is MOST important in the development of:

- ☒ strategic plans.
- ☐ IS policies.
- ☐ IS procedures.
- ☐ standards and guidelines.

Explanation:

Explanation:

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

Licensed to Berend Post berend.post@it-university.nl

Question 1954

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- ☐ Halon gas
- ☐ Wet-pipe sprinklers
- ☒ Dry-pipe sprinklers
- ☐ Carbon dioxide gas

Explanation:

Explanation: Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat to life, and water is environmentally friendly.

Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

Question 1955

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

- ☒ The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
- ☐ The service provider does not have incident handling procedures.
- ☐ Recently a corrupted database could not be recovered because of library management problems.
- ☐ incident logs are not being reviewed.

Explanation:

Explanation:

The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

Licensed to Berend Post berend.post@it-university.nl

Question 1956

Responsibility and reporting lines cannot always be established when auditing automated systems since:

- ☐ diversified control makes ownership irrelevant.
- ☐ staff traditionally changes jobs with greater frequency.
- ☒ ownership is difficult to establish where resources are shared.
- ☐ duties change frequently in the rapid development of technology.

Explanation:

Explanation:

Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

Question 1957

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

- ☐ Time zone differences could impede communications between IT teams.
- ☐ Telecommunications cost could be much higher in the first year.
- ☒ Privacy laws could prevent cross-border flow of information.
- ☐ Software development may require more detailed specifications.

Explanation:

Explanation:

Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

Question 1958

An objective of capacity management is to ensure that:

- ☒ organizational resources are used efficiently.
- ☐ available resources are fully utilized.
- ☐ new resources are allocated for new applications.
- ☐ resource utilization does not drop below 85%.

Licensed to Berend Post berend.post@it-university.nl

Question 1959

An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

- ☐ Program evaluation review technique (PERT)
- ☐ Counting source lines of code (SLOC)
- ☒ Function point analysis
- ☐ White box testing

Explanation:

Explanation:

Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications. PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

Question 1960

An online retailer is receiving customer about receiving different items from what they ordered on the organization's website. The root cause has been traced to poor data quality. Despite efforts to clean erroneous data from the system, multiple data quality issues continue to occur. Which of the following recommendations would be the BEST way to reduce the likelihood of future occurrences?

- ☒ Implement business rules to validate employee data entry.
- ☐ Invest in additional employee training for data entry.
- ☐ Assign responsibility for improving data quality.
- ☐ Outsource data cleansing activities to reliable third parties.

Question 1961

If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

- ☐ Documentation development
- ☒ Comprehensive integration testing
- ☐ Full unit testing
- ☐ Full regression testing

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

If an IS auditor observes individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further comprehensive integration testing.

Question 1962

An IS audit of an organization's data classification policies finds some areas of the policies may not be up-to-date with new data privacy regulations. What should management do FIRST to address the risk of noncompliance?

- ☒ Conduct a privacy impact assessment to identify gaps
- ☐ Reclassify information based on revised information classification labels
- ☐ Mandate training on the new privacy regulations
- ☐ Perform a data discovery exercise to identify all personal data

Question 1963

The MOST important reason that security risk assessment should be conducted frequently throughout an organization is because:

- ☒ threats to the organization may change.
- ☐ controls should be regularly tested.
- ☐ compliance with legal and regulatory standards should be reassessed.
- ☐ control effectiveness may weaken.

Question 1964

Which of the following are examples of tools for launching Distributed DoS Attack (Choose four.):

- ☒ TFN
- ☒ TFN2K
- ☒ Trin00
- ☒ Stacheldracht
- ☐ Tripwire

Explanation:

Explanation:

Distributed DoS Attack is a network-based attack from many servers used remotely to send packets. Examples of tools for conducting such attack include TFN, TFN2K, Trin00, Stacheldracht, and variants. The best defense is to make sure all systems patches are up-to-date. Also make sure your firewalls are configured appropriately.

Licensed to Berend Post berend.post@it-university.nl

Question 1965

For mission-critical applications with a low recovery time objective (RTO), which of the following is the BEST backup strategy?

- ☐ Frequent back-ups to tape
- ☒ Mirroring
- ☐ Use of virtual tape libraries
- ☐ Archiving to conventional disk

Question 1966

Which of the following is the MOST important prerequisite to performing an information security assessment?

- ☐ Reviewing the business impact analysis (BIA)
- ☐ Assessing threats and vulnerabilities
- ☐ Determining risk tolerance
- ☒ Classifying assets

Question 1967

Which of the following is MOST important when planning a network audit?

- ☐ Determination of IP range in use
- ☐ Isolation of rogue access points
- ☒ Identification of existing nodes
- ☐ Analysis of traffic content

Question 1968

Which of the following is the MOST important feature of access control software?

- ☒ Authentication
- ☐ Violation reporting
- ☐ Nonrepudiation
- ☐ Identification

Licensed to Berend Post berend.post@it-university.nl

Question 1969

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

- ☐ security requirements for the process being outsourced
- ☐ security metrics
- ☒ service level agreements (SLAs)
- ☐ risk-reporting methodologies

Question 1970

An organization implements a data loss prevention tool as a control to mitigate the risk of sensitive data leaving the organization via electronic mail. Which of the following would provide the BEST indication of adequate control design?

- ☐ Management has formally approved the control design.
- ☐ Management presents evidence that data loss incidents have decreased.
- ☒ Security administrators can demonstrate the functions of the tool.
- ☐ Rules enforced by the tool were based on the classification of the data.

Question 1971

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

Question 1972

In RFID technology which of the following risk could represent a threat to non-RFID networked or collocated systems, assets, and people?

- ☐ Business Process Risk
- ☐ Business Intelligence Risk
- ☐ Privacy Risk
- ☒ Externality Risk

Explanation:

RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

Licensed to Berend Post berend.post@it-university.nl

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person.

Externality risks are present for both the RF and enterprise subsystems of an RFID system.

The main externality risk for the RF subsystem is hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance.

The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage.

The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application. Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

For your exam you should know the information below:

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

Licensed to Berend Post berend.post@it-university.nl

RFID technology enables an organization to significantly change its business processes to:

Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 248

Question 1973

Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

- ☐ System patcher
- ☒ Porn dialer
- ☐ War dialer
- ☐ T1 dialer
- ☐ T3 dialer
- ☐ None of the choices.

Explanation:

Explanation:

One way of stealing money from infected PC owner is to take control of the modem and dial an expensive toll call. Dialer such as porn dialer software dials up a premium-rate telephone number and leave the line open, charging the toll to the infected user.

Licensed to Berend Post berend.post@it-university.nl

Question 1974

Which of the following would provide the MOST reliable evidence to indicate whether employee access has been deactivated in a timely manner following termination?

- ☐ Comparing termination forms with dates in the HR system
- ☐ Reviewing hardware return-of-asset forms
- ☐ Interviewing supervisors to verify employee data is being updated immediately
- ☒ Comparing termination forms with system transaction log entries

Question 1975

Which of the following should be the GREATEST concern to an IS auditor reviewing the information security framework of an organization?

- ☐ The information security policy has not been updated in the last two years.
- ☒ A list of critical information assets was not included in the information security policy.
- ☐ Senior management was not involved in the development of the information security policy.
- ☐ The information security policy is not aligned with regulatory requirements.

Question 1976

Which of the following is necessary to determine what would constitute a disaster for an organization?

- ☐ Backup strategy analysis
- ☐ Threat probability analysis
- ☐ Risk analysis
- ☒ Recovery strategy analysis

Question 1977

Which of the following would be the MOST effective method to identify high risk areas in the business to be included in the audit plan?

- ☐ Validate current risk from prior internal audit findings.
- ☐ Review industry reports to identify common risk areas.
- ☐ Engage with management to understand the business.
- ☒ Review external audit reports of the business.

Licensed to Berend Post berend.post@it-university.nl

Question 1978

Gimmes often work through:

- ☐ SMS
- ☐ IRC chat
- ☒ email attachment
- ☐ news
- ☐ file download
- ☐ None of the choices.

Explanation:

Explanation:

Gimmes take advantage of curiosity or greed to deliver malware. Also known as a Trojan Horse, gimmes can arrive as an email attachment promising anything. The recipient is expected to give in to the need to the program and open the attachment. In addition, many users will blindly click on any attachments they receive that seem even mildly legitimate.

Question 1979

Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

- ☐ There are three individuals with a key to enter the area.
- ☐ Paper documents are also stored in the offsite vault.
- ☒ Data files that are stored in the vault are synchronized.
- ☐ The offsite vault is located in a separate facility.

Explanation:

Explanation:

Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

Question 1980

An effective implementation of security roles and responsibilities is BEST evidenced across an enterprise when:

- ☒ operational activities are aligned with policies.
- ☐ policies are signed off by users.
- ☐ policies are rolled out and disseminated.
- ☐ reviews and updates of policies are regularly performed.

Licensed to Berend Post berend.post@it-university.nl

Question 1981

Which of the following should occur EARLIEST in a business continuity management lifecycle?

- ☐ Defining business continuity procedures
- ☐ Identifying critical business processes
- ☐ Developing a training and awareness program
- ☒ Carrying out a threat and risk assessment

Question 1982

An internal audit department recently established a quality assurance (QA) program as part of its overall audit program. Which of the following activities should be included as part of the QA program requirements?

- ☐ Reporting program results to the board
- ☒ Reviewing audit standards periodically
- ☐ Analyzing user satisfaction reports from business lines
- ☐ Conducting long-term planning for internal audit staffing

Question 1983

During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

- ☒ buffer overflow.
- ☐ brute force attack.
- ☐ distributed denial-of-service attack.
- ☐ war dialing attack.

Explanation:

Explanation:

Poorly written code, especially in web-based applications, is often exploited by hackers using buffer overflow techniques. A brute force attack is used to crack passwords. A distributed denial- of-service attack floods its target with numerous packets, to prevent it from responding to legitimate requests. War dialing uses modem-scanning tools to hack PBXs.

Licensed to Berend Post berend.post@it-university.nl

Question 1984

Which of the following would be MOST important for an IS auditor to review during an audit of an automated continuous monitoring process being used by the finance department?

- ☐ Resiliency of the monitoring service
- ☒ Dual control and approvals embedded in processes
- ☐ Management sign-off of test documentation
- ☐ Configuration of the monitoring tool

Question 1985

How does the SSL network protocol provide confidentiality?

- ☐ Through symmetric encryption such as RSA
- ☐ Through asymmetric encryption such as Data Encryption Standard, or DES
- ☐ Through asymmetric encryption such as Advanced Encryption Standard, or AES
- ☒ Through symmetric encryption such as Data Encryption Standard, or DES

Explanation:

Explanation:

The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption.

Standard, or DES.

Question 1986

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- ☒ business plan.
- ☐ audit plan.
- ☐ security plan.
- ☐ investment plan.

Explanation:

Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

Licensed to Berend Post berend.post@it-university.nl

Question 1987

Which of the following is the PRIMARY purpose for conducting parallel testing?

- ☐ To determine if the system is cost-effective
- ☐ To enable comprehensive unit and system testing
- ☐ To highlight errors in the program interfaces with files
- ☒ To ensure the new system meets user requirements

Explanation:

Explanation:

The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements. Parallel testing may show that the old system is, in fact, better than the new system, but this is not the primary reason. Unit and system are completed before parallel testing. Program interfaces with files are tested for errors during system testing.

Question 1988

Cross-site scripting (XSS) attacks are BEST prevented through:

- ☐ use of common industry frameworks.
- ☒ secure coding practices.
- ☐ application firewall policy settings.
- ☐ a three-tier web architecture.

Question 1989

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

- ☐ Business interruption
- ☒ Fidelity coverage
- ☐ Errors and omissions
- ☐ Extra expense

Explanation:

Explanation:

Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

Licensed to Berend Post berend.post@it-university.nl

Question 1990

In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

- ☐ Reporting
- ☐ Attacks
- ☒ Discovery
- ☐ Planning

Question 1991

In the context of physical access control, what is known as the process of verifying user identities?

- ☒ Authentication
- ☐ Authorization
- ☐ Accounting
- ☐ Encryption
- ☐ Compression
- ☐ None of the choices.

Explanation:

Explanation:

Authentication is the process of verifying a user's claimed identity. It is based on at least one of these three factors: Something you know, Something you have, or Something you are.

Question 1992

During the audit of a database server, which of the following would be considered the GREATEST exposure?

- ☐ The password does not expire on the administrator account
- ☒ Default global security settings for the database remain unchanged
- ☐ Old data have not been purged
- ☐ Database activity is not fully logged

Explanation:

Explanation:

Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

Licensed to Berend Post berend.post@it-university.nl

Question 1993

What is the FIRST step an auditor should take when beginning a follow-up audit?

- ☐ Review workpapers from the previous audit.
- ☐ Gather evidence of remediation to conduct tests of controls.
- ☒ Review previous findings and action plans.
- ☐ Meet with the auditee to discuss remediation progress.

Question 1994

A database administrator is responsible for:

- ☐ defining data ownership.
- ☐ establishing operational standards for the data dictionary.
- ☒ creating the logical and physical database.
- ☐ establishing ground rules for ensuring data integrity and security.

Explanation:

Explanation:

A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

Question 1995

Which of the following tools BEST demonstrate the effectiveness of the information security program?

- ☒ A security balanced scorecard
- ☐ Management satisfaction surveys
- ☐ Risk heat map
- ☐ Key risk indicators (KRIs)

Question 1996

Which of the following is the BEST way to increase the effectiveness of security incident detection?

- ☐ Determining containment activities based on the type of incident
- ☐ Establishing service level agreements (SLAs) with appropriate forensic service providers
- ☐ Educating end users on identifying suspicious activity
- ☒ Documenting root cause analysis procedures

Licensed to Berend Post berend.post@it-university.nl

Question 1997

You should keep all computer rooms at reasonable humidity levels, which are in between:

- ☒ 20 - 70 percent.
- ☐ 10 - 70 percent.
- ☐ 10 - 60 percent.
- ☐ 70 - 90 percent.
- ☐ 60 - 80 percent.
- ☐ None of the choices.

Explanation:

Explanation:

You should keep all computer rooms at reasonable temperatures, which is in between 60 - 75 degrees Fahrenheit or 10 - 25 degrees Celsius. You should also keep humidity levels at 20 - 70 percent.

Question 1998

Which of the following is the MOST significant risk associated with the use of virtualization?

- ☐ Insufficient network bandwidth
- ☐ Single point of failure
- ☐ Inadequate configuration
- ☒ Performance issues of hosts

Question 1999

Which of the following would be BEST prevented by a raised floor in the computer machine room?

- ☒ Damage of wires around computers and servers
- ☐ A power failure from static electricity
- ☐ Shocks from earthquakes
- ☐ Water flood damage.

Explanation:

Explanation:

The primary reason for having a raised floor is to enable power cables and data cables to be installed underneath the floor. This eliminates the safety and damage risks posed when cables are placed in a spaghetti-like fashion on an open floor. Static electricity should be avoided in the machine room; therefore, measures such as specially manufactured carpet or shoes would be more appropriate for static prevention than a raised floor. Raised floors do not address shocks from earthquakes. To address earthquakes, anti-seismic architecture would be required to establish a quake-resistant structural framework. Computer equipment needs to be protected against water. However, a raised floor would not prevent damage to the machines in the event of overhead water pipe leakage.

Licensed to Berend Post berend.post@it-university.nl

Question 2000

A data breach has occurred at a third-party vendor used by an organization to outsource the processing of its customer data. What should be management's FIRST course of action?

- ☐ Activate the disaster recovery plan
- ☐ Notify the insurance company of the potential claim
- ☒ Activate the incident management process
- ☐ Take legal action against the service provider for reputation damage

Question 2001

An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

- ☒ encrypting the hash of the newsletter using the advisor's private key.
- ☐ encrypting the hash of the newsletter using the advisor's public key.
- ☐ digitally signing the document using the advisor's private key.
- ☐ encrypting the newsletter using the advisor's private key.

Explanation:

Explanation:

There is no attempt on the part of the investment advisor to prove their identity or to keep the newsletter confidential. The objective is to assure the receivers that it came to them without any modification, i.e., it has message integrity. Choice A is correct because the hash is encrypted using the advisor's private key. The recipients can open the newsletter, recompute the hash and decrypt the received hash using the advisor's public key. If the two hashes are equal, the newsletter was not modified in transit. Choice B is not feasible, for no one other than the investment advisor can open it. Choice C addresses sender authentication but not message integrity. Choice D addresses confidentiality, but not message integrity, because anyone can obtain the investment advisor's public key, decrypt the newsletter, modify it and send it to others. The interceptor will not be able to use the advisor's private key, because they do not have it.

Anything encrypted using the interceptor's private key can be decrypted by the receiver only by using their public key.

Question 2002

Requiring that passwords contain a combination of numeric and alphabetic characters is MOST effective against which type of attack?

- ☐ Denial of service
- ☒ Dictionary
- ☐ Social engineering
- ☐ Programmed

Licensed to Berend Post berend.post@it-university.nl

Question 2003

A client/server configuration will:

- ☒ optimize system performance by having a server on a front-end and clients on a host
- ☐ enhance system performance through the separation of front-end and back-end processes
- ☐ keep track of all the clients using the IS facilities of a service organization
- ☐ limit the clients and servers' relationship by limiting the IS facilities to a single hardware system

Question 2004

Which of the following function in traditional EDI process is used for transmitting and receiving electronic documents between trading partners via dial up lines, public switched network or VAN?

- ☒ Communication handler
- ☐ EDI Interface
- ☐ Application System
- ☐ EDI Translator

Explanation:

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN).

For your exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's computer system

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox services similar to post offices. The VAN receives all the outbound transactions from an organization, sort them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

EDI Interface -Interface function that manipulates and routes data between the application system and the communication handler. The interface consists of two components

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Licensed to Berend Post berend.post@it-university.nl

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping. Data mapping is the process by which data are extracted from EDI translation process and integrated with the data or process of receiving company.

3. Application System -The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

EDI Interface -Interface function that manipulates and routes data between the application system and the communication handler.

Application System -The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

EDI Translator- The device translates data between standard format (ANSI X12) and trading partner's propriety information.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 178

Question 2005

What should be the PRIMARY objective of conducting interviews with business unit managers when developing an information security strategy?

- ☒ Obtain information on department goals.
- ☐ Classify information assets.
- ☐ Identify data and system ownership.
- ☐ Determine information types.

Licensed to Berend Post berend.post@it-university.nl

Question 2006

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

- ☐ scheduling may be performed months in advance.
- ☐ budgets are more likely to be met by the IS audit staff.
- ☐ staff will be exposed to a variety of technologies.
- ☒ resources are allocated to the areas of highest concern

Explanation:

Explanation:

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

Question 2007

An employee loses a mobile device resulting in loss of sensitive corporate data. Which of the following would have BEST prevented data leakage?

- ☐ Awareness training for mobile device users
- ☐ Data encryption on the mobile device
- ☒ The triggering of remote data wipe capabilities
- ☐ Complex password policy for mobile devices

Question 2008

Which of the following is necessary for the effective risk management in IT governance?

- ☒ Risk evaluation is embedded in management processes
- ☐ Risk management strategy is approved by the audit committee
- ☐ Local managers are solely responsible for risk evaluation
- ☐ IT risk management is separate from corporate risk management

Licensed to Berend Post berend.post@it-university.nl

Question 2009

To help ensure the organization's information assets are adequately protected, which of the following considerations is MOST important when developing an information classification and handling policy?

- ☐ The policy has been mapped against industry frameworks for classifying information assets.
- ☐ The policy is owned by the head of information security, who has the authority to enforce the policy.
- ☐ The policy specifies requirements to safeguard information assets based on their importance to the organization.
- ☒ The policy is subject to periodic reviews to ensure its provisions are up to date.

Question 2010

Which of the following would be the GREATEST concern to an IS auditor reviewing an IT outsourcing arrangement?

- ☒ Several IT personnel perform the same functions as the vendor.
- ☐ The contract does not include a renewal option.
- ☐ Development of KPIs that will be used was assigned to the vendor.
- ☐ Some penalties were waived during contract negotiations.

Question 2011

Which of the following option INCORRECTLY describes PBX feature?

- ☐ Voice mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
- ☒ Tenanting-Provides for the possibility to break into a busy line to inform another user an important message
- ☐ Automatic Call Distribution - Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available
- ☐ Diagnostics -Allows for bypassing normal call restriction procedures

Explanation:

The word INCORRECTLY was the keyword used in the question. You need to find out the incorrectly described PBX feature from given options. The Tenanting feature is incorrectly described.

Tenanting limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

For your exam you should know below mentioned PBX features and Risks:

Licensed to Berend Post berend.post@it-university.nl

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking

Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)

Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes

Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features

Silent Monitoring

Licensed to Berend Post berend.post@it-university.nl

Silently monitors other calls

Eavesdropping

Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference

override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping

Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting

Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail

Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Licensed to Berend Post berend.post@it-university.nl

Privacy release

Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics

Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting

When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

The other options presented correctly describes PBX features thus not the right choice.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number358

Question 2012

Which of the following is MOST likely to be prevented by a firewall connected to the Internet?

- ☐ Dial-in penetration attacks
- ☒ Disclosure of public key infrastructure (PKI) keys
- ☐ Alteration of email message content
- ☐ External spoofing of internal addresses

Question 2013

The security level of a private key system depends on the number of:

- ☒ encryption key bits.
- ☐ messages sent.
- ☐ keys.
- ☐ channels used.

Explanation:

Explanation:

The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

Question 2014

An accuracy measure for a biometric system is:

- ☐ system response time.
- ☐ registration time.
- ☐ input file size.
- ☒ false-acceptance rate.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

For a biometric solution three main accuracy measures are used: false-rejection rate (FRR), cross-error rate (CER) and false-acceptance rate (FAR). FRR is a measure of how often valid individuals are rejected. FAR is a measure of how often invalid individuals are accepted. CER is a measure of when the false-rejection rate equals the false-acceptance rate. Choices A and B are performance measures.

Question 2015

Who is ultimately accountable for the development of an IS security policy?

- ☒ The board of directors
- ☐ Middle management
- ☐ Security administrators
- ☐ Network administrators

Explanation:

Explanation:

The board of directors is ultimately accountable for the development of an IS security policy.

Question 2016

An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- ☐ Electromagnetic interference (EMI)
- ☐ Cross-talk
- ☐ Dispersion
- ☒ Attenuation

Explanation:

Explanation:

Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMI) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

Licensed to Berend Post berend.post@it-university.nl

Question 2017

Which of the following should be of MOST concern to an IS auditor reviewing an organization's disaster recovery plan (DRP)?

- ☐ The responsibility for declaring a disaster is not identified.
- ☒ The disaster recovery steps are not detailed.
- ☐ The CIO has not signed off on the DRP.
- ☐ Copies of the DRP are not kept in a secure offsite location.

Question 2018

Which of the following is the BEST IS audit strategy?

- ☒ Perform audits based on impact and probability of error and failure.
- ☐ Cycle general control and application audits over a two-year period.
- ☐ Conduct general control audits annually and application audits in alternating years.
- ☐ Limit audits to new application system developments.

Question 2019

Which of the following statement INCORRECTLY describes the traditional audit approach in comparison to the Control self-assessment approach?

- ☒ In traditional approach, Staffs at all level, in all functions, are the primary control analyst.
- ☐ Traditional approach assigns duties/supervises staff
- ☐ Traditional approach is a policy driven approach
- ☐ Traditional approach requires limited employee participations.

Explanation:

Explanation:

The keyword INCORRECTLY is used in the question. You need to find out an option which incorrectly describes the traditional approach.

For your exam you should know the information below about control self-assessment and traditional approach:

The traditional approach can be summarized as any approach in which the primary responsibility for analyzing and reporting on internal control and risk is assigned to auditor and to lesser extent, controller department and outside consultants.

Control self-assessment is an assessment of controls made by the staff and management of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal controls of the organization are reliable.

Licensed to Berend Post berend.post@it-university.nl

Benefits of CSA

Early detection of risk

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives

Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

Highly motivated employees

Improved audit training process

Reduction in control cost

Assurance provided to stakeholders and customers

Traditional and CSA attributes

Traditional Historical CSA

Assign duties/supervises staff Empowered/accountable employees

Policy/rule driven Continuous improvement/learning curve

Limited employee participation Extensive employee participation and training

Narrow stakeholders focus Broad stakeholders focus

Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are correctly describes about traditional approach.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 61, 62 and 63

Licensed to Berend Post berend.post@it-university.nl

Question 2020

Which of the following should be the GREATEST concern to an IS auditor evaluating an organization's policies?

- ☐ Policies are not formally approved by the management.
- ☐ Policies are nor formally acknowledged and signed by employees.
- ☒ Policies do not provide adequate protection to the organization.
- ☐ Policies are not reviewed and updated frequently.

Question 2021

Which of the following may be deployed in a network as lower cost surveillance and early-warning tools?

- ☒ Honeypots
- ☐ Hardware IPSs
- ☐ Hardware IDSs
- ☐ Botnets
- ☐ Stateful inspection firewalls
- ☐ Stateful logging facilities
- ☐ None of the choices.

Explanation:

Explanation:

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques.

Question 2022

What is the MOST important role of a Certificate Authority (CA) when a private key becomes compromised?

- ☐ Issue a new private key to the user
- ☐ Refresh the key information database in the certificate publishing server
- ☒ Publish the certificate revocation lists (CRL) into the repository
- ☐ Refresh the metadata of the certificates

Licensed to Berend Post berend.post@it-university.nl

Question 2023

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- ☒ complexity and risks associated with the project have been analyzed.
- ☐ resources needed throughout the project have been determined.
- ☐ project deliverables have been identified.
- ☐ a contract for external parties involved in the project has been completed.

Explanation:

Explanation:

Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome. The other choices, while important during the course of the project, cannot be fully determined at the time the project is initiated, and are often contingent upon the risk and complexity of the project.

Question 2024

When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

- ☐ Read access to data
- ☒ Delete access to transaction data files
- ☐ Logged read/execute access to programs
- ☐ Update access to job control language/script files

Explanation:

Explanation:

Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL to control job execution.

Question 2025

Sophisticated database systems provide many layers and types of security, including (Choose three.):

- ☒ Access control
- ☒ Auditing
- ☒ Encryption
- ☒ Integrity controls
- ☐ Compression controls

Explanation:

Explanation:

Sophisticated database systems provide many layers and types of security, including Access control, Auditing, Authentication, Encryption and Integrity controls. An important procedure when evaluating

Licensed to Berend Post berend.post@it-university.nl

database security is performing vulnerability assessments against the database. Database administrators or Information security administrators run vulnerability scans on databases to discover misconfiguration of controls within the layers mentioned above along with known vulnerabilities within the database software.

Question 2026

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

- ☐ An oral statement from the auditee
- ☐ The results of a test performed by an IS auditor
- ☐ An internally generated computer accounting report
- ☒ A confirmation letter received from an outside source

Explanation:

Explanation:

Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

Question 2027

When reviewing the configuration of network devices, an IS auditor should FIRST identify:

- ☐ the best practices for the type of network devices deployed.
- ☐ whether components of the network are missing.
- ☒ the importance of the network device in the topology.
- ☐ whether subcomponents of the network are being used appropriately.

Explanation:

Explanation:

The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for deployment of the device in the network.

Licensed to Berend Post berend.post@it-university.nl

Question 2028

An IS auditor should be concerned when a telecommunication analyst:

- ☒ monitors systems performance and tracks problems resulting from program changes.
- ☐ reviews network load requirements in terms of current and future transaction volumes.
- ☐ assesses the impact of the network load on terminal response times and network data transfer rates.
- ☐ recommends network balancing procedures and improvements.

Explanation:

Explanation:

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes {choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes {choice A) would put the analyst in a self- monitoring role.

Question 2029

What influences decisions regarding criticality of assets?

- ☐ The business criticality of the data to be protected
- ☐ Internal corporate politics
- ☒ The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
- ☐ The business impact analysis

Explanation:

Explanation:

Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

Question 2030

An information security manager learns that a departmental system is out of compliance with the information security policy's authentication requirements. Which of the following should be the information security manager's FIRST course of action?

- ☐ Isolate the noncompliant system from the rest of the network.
- ☐ Submit the issue to the steering committee for escalation.
- ☐ Request risk acceptance from senior management.
- ☒ Conduct an impact analysis to quantify the associated risk.

Licensed to Berend Post berend.post@it-university.nl

Question 2031

Which of the following provides the BEST evidence of successfully completed batch uploads?

- ☐ Sign-off on the batch journal
- ☒ Using sequence controls
- ☐ Enforcing batch cut-off times
- ☐ Reviewing process logs

Question 2032

Which of the following protocol is developed jointly by VISA and Master Card to secure payment transactions among all parties involved in credit card transactions on behalf of cardholders and merchants?

- ☐ S/MIME
- ☐ SSH
- ☒ SET
- ☐ S/HTTP

Explanation:

Secure Electronic Transaction(SET) is a protocol developed jointly by VISA and Master Card to secure payment transaction among all parties involved in credit card transactions among all parties involved in credit card transactions on behalf of cardholders and merchants. As an open system specification, SET is an application-oriented protocol that uses trusted third party's encryption and digital-signature process, via PKI infrastructure of trusted third party institutions, to address confidentiality of information, integrity of data, cardholders authentication, merchant authentication and interoperability.

The following were incorrect answers:

S/MIME - Secure Multipurpose Internet Mail Extension (S/MIME) is a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of message's content's, including attachments.

SSH –A client server program that opens a secure, encrypted command-line shell session from the Internet for remote logon. Similar to a VPN, SSH uses strong cryptography to protect data, including password, binary files and administrative commands, transmitted between system on a network. SSH is typically implemented between two parties by validating each other's credential via digital certificates. SSH is useful in securing Telnet and FTP services, and is implemented at the application layer, as opposed to operating at network layer (IPSec Implementation)

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type

Licensed to Berend Post berend.post@it-university.nl

connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352 and 353

Question 2033

Which of the following is MOST likely to result from compliance testing?

- ☐ Comparison of data with physical counts
- ☐ Confirmation of data with outside sources
- ☐ Identification of errors due to processing mistakes
- ☒ Discovery of controls that have not been applied

Question 2034

Which type of risk would MOST influence the selection of a sampling methodology?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☒ Detection

Question 2035

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

- ☐ evaluate the record retention plans for off-premises storage.
- ☒ interview programmers about the procedures currently being followed.
- ☐ compare utilization records to operations schedules.
- ☐ review data file access records to test the librarian function.

Explanation:

Explanation:

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the

access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

Licensed to Berend Post berend.post@it-university.nl

Question 2036

In which of the following RFID risks competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system?

- ☐ Business Process Risk
- ☒ Business Intelligence Risk
- ☐ Privacy Risk
- ☐ Externality Risk

Explanation:

An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

RFID is a powerful technology, in part, because it supports wireless remote access to information about assets and people that either previously did not exist or was difficult to create or dynamically maintain. While this wireless remote access is a significant benefit, it also creates a risk that unauthorized parties could also have similar access to that information if proper controls are not in place. This risk is distinct from the business process risk because it can be realized even when business processes are functioning as intended.

A competitor or adversary can gain information from the RFID system in a number of ways, including eavesdropping on RF links between readers and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to a back-end database storing information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases.

The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information. In some cases, the information may trigger an immediate response. For example, someone might use a reader to determine whether a shipping container holds expensive electronic equipment, and then break into the container when it gets a positive reading. This scenario is an example of targeting. In other cases, data might also be aggregated over time to provide intelligence regarding an organization's operations, business strategy, or proprietary methods.

For instance, an organization could monitor the number of tags entering a facility to provide a reasonable indication of its business growth or operating practices. In this case, if someone determined that a warehouse recently received a number of very large orders, then that might trigger an action in financial markets or prompt a competitor to change its prices or production schedule.

For your exam you should know the information below:

Licensed to Berend Post berend.post@it-university.nl

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to:

Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Licensed to Berend Post berend.post@it-university.nl

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 248

Licensed to Berend Post berend.post@it-university.nl

Question 2037

When developing a security architecture, which of the following steps should be executed FIRST?

- ☐ Developing security procedures
- ☒ Defining a security policy
- ☐ Specifying an access control methodology
- ☐ Defining roles and responsibilities

Explanation:

Explanation:

Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies will often set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

Question 2038

The Federal Information Processing Standards (FIPS) were developed by:

- ☒ the United States Federal government
- ☐ ANSI
- ☐ ISO
- ☐ IEEE
- ☐ IANA
- ☐ None of the choices.

Explanation:

Explanation:

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all nonmilitary government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community.

Licensed to Berend Post berend.post@it-university.nl

Question 2039

What should an organization do before providing an external agency physical access to its information processing facilities (IPFs)?

- ☐ The processes of the external agency should be subjected to an IS audit by an independent agency.
- ☐ Employees of the external agency should be trained on the security procedures of the organization.
- ☐ Any access by an external agency should be limited to the demilitarized zone (DMZ).
- ☒ The organization should conduct a risk assessment and design and implement appropriate controls.

Explanation:

Explanation:

Physical access of information processing facilities (IPFs) by an external agency introduces additional threats into an organization. Therefore, a risk assessment should be conducted and controls designed accordingly. The processes of the external agency are not of concern here. It is the agency's interaction with the organization that needs to be protected. Auditing their processes would not be relevant in this scenario. Training the employees of the external agency may be one control procedure, but could be performed after access has been granted. Sometimes an external agency may require access to the processing facilities beyond the demilitarized zone (DMZ). For example, an agency which undertakes maintenance of servers may require access to the main server room. Restricting access within the DMZ will not serve the purpose.

Question 2040

The BEST way to obtain funding from senior management for a security awareness program is to:

- ☐ meet regulatory requirements
- ☒ produce an impact analysis report of potential breaches
- ☐ demonstrate that the program will adequately reduce risk
- ☐ produce a report of organizational risks

Question 2041

Which of the following is the PRIMARY objective of an IT performance measurement process?

- ☐ Minimize errors
- ☐ Gather performance data
- ☐ Establish performance baselines
- ☒ Optimize performance

Explanation:

Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an

Licensed to Berend Post berend.post@it-university.nl

aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

Question 2042

Reviewing project plans and status reports throughout the development life cycle will:

- ☐ eliminate the need to perform a risk assessment.
- ☐ postpone documenting the project's progress until the final phase.
- ☐ guarantee that the project will meet its intended deliverables.
- ☒ facilitate the optimal use of resources over the life of the project.

Question 2043

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization's backup processes?

- ☐ A written backup policy is not available.
- ☐ Backup failures are not resolved in a timely manner.
- ☐ The restoration process is slow due to connectivity issues.
- ☒ The service levels are not achieved.

Question 2044

A trojan horse simply cannot operate autonomously.

- ☒ true
- ☐ false

Explanation:

Explanation:

As a common type of Trojan horses, a legitimate software might have been corrupted with malicious code which runs when the program is used. The key is that the user has to invoke the program in order to trigger the malicious code. In other words, a trojan horse simply cannot operate autonomously. You would also want to know that most but not all trojan horse payloads are harmful - a few of them are harmless.

Licensed to Berend Post berend.post@it-university.nl

Question 2045

Which of the following type of IDS has self-learning functionality and over a period of time will learned what is the expected behavior of a system?

- ☐ Signature Based IDS
- ☐ Host Based IDS
- ☒ Neural Network based IDS
- ☐ Statistical based IDS

Explanation:

Neural Network based IDS monitors the general patterns of activity and traffic on the network, and create a database of normal activities within the system. This is similar to statistical model but with added self-learning functionality.

Also, you should know below categories and types of IDS for CISA exam:

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies.

Broad category of IDS includes:

Network based IDS

Host based IDS

Network Based IDS

They identify attack within the monitored network and issue a warning to the operator.

If a network based IDS is placed between the Internet and the firewall, it will detect all the attack attempts whether or not they enter the firewall

Host Based IDS

They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack.

They can detect the modification of executable programs, detect the detection of files and issue a warning when an attempt is made to use a privilege account.

Licensed to Berend Post berend.post@it-university.nl

Types of IDS includes

Signature Based IDS – These IDS system protect against detected intrusion patterns. The intrusive pattern they can identify are stored in the form of signature.

Statistical Based IDS – This system needs a comprehensive definition of the known and expected behavior of system

Neural Network – An IDS with this feature monitors the general patterns of activity and traffic on the network, and create a database. This is similar to statistical model but with added self-learning functionality

The following were incorrect answers:

The other types of IDS mentioned in the options do not monitor general patterns of activities and contains self-learning functionalities.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 346 and 347

Question 2046

Which of the following should be included in an organization's IS security policy?

- ☐ A list of key IT resources to be secured
- ☒ The basis for access authorization
- ☐ Identity of sensitive security features
- ☐ Relevant software security features

Explanation:

Explanation:

The security policy provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

Licensed to Berend Post berend.post@it-university.nl

Question 2047

A virtual private network (VPN) provides data confidentiality by using:

- ☐ Secure Sockets Layer (SSL)
- ☒ Tunneling
- ☐ Digital signatures
- ☐ Phishing

Explanation:

Explanation:

VPNs secure data in transit by encapsulating traffic, a process known as tunneling. SSL is a symmetric method of encryption between a server and a browser. Digital signatures are not used in the VPN process, while phishing is a form of a social engineering attack.

Question 2048

What is the primary objective of a control self-assessment (CSA) program?

- ☒ Enhancement of the audit responsibility
- ☐ Elimination of the audit responsibility
- ☐ Replacement of the audit responsibility
- ☐ Integrity of the audit responsibility

Explanation:

Explanation:

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

Question 2049

Which of the following is the MOST effective way to maintain network integrity when using mobile devices?

- ☐ Perform network reviews.
- ☒ Implement network access control.
- ☐ Implement outbound firewall rules.
- ☐ Review access control lists.

Licensed to Berend Post berend.post@it-university.nl

Question 2050

A data administrator is responsible for:

- ☐ maintaining database system software.
- ☒ defining data elements, data names and their relationship.
- ☐ developing physical database structures.
- ☐ developing data dictionary system software.

Explanation:

Explanation:

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

Question 2051

Which of the following is the MOST effective control to mitigate unintentional misuse of authorized access?

- ☐ Regular monitoring of user access logs
- ☐ Annual sign-off of acceptable use policy
- ☒ Security awareness training
- ☐ Formalized disciplinary action

Question 2052

Most trojan horse programs are spread through:

- ☒ e-mails.
- ☐ MP3.
- ☐ MS Office.
- ☐ Word template.
- ☐ None of the choices.

Explanation:

Explanation:

"Most trojan horse programs are spread through e-mails. Some earlier trojan horse programs were bundled in "Root Kits". For example, the Linux Root Kit version 3 (lrk3) which was released in December 96 had tcp wrapper trojans included and enhanced in the kit. Portable devices that run Linux can also be affected by trojan horse. The Trojan.Linux.JBellz Trojan horse runs as a malformed .mp3 file."

Licensed to Berend Post berend.post@it-university.nl

Question 2053

During a follow-up audit, an IS auditor finds that the auditee has updated virus scanner definitions without adopting the original audit recommendation to increase the frequency of using the scanner. The MOST appropriate action for the auditor is to:

- ☐ prepare a follow-up audit report reiterating the recommendation.
- ☐ escalate the issue to senior management.
- ☒ modify the audit opinion based on the new information available.
- ☐ conclude that the residual risk is beyond tolerable levels of risk.

Question 2054

Software quality assurance (QA) reviews are planned as part of system development. At which stage in the development process should the first review be initiated?

- ☐ At pre-implementation planning
- ☐ As a part of the user requirements definition
- ☐ Immediately prior to user acceptance testing
- ☒ During the feasibility study

Question 2055

Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

Question 2056

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager to perform?

- ☐ Identity unacceptable risk levels
- ☒ Manage the impact
- ☐ Evaluate potential threats
- ☐ Assess vulnerabilities

Licensed to Berend Post berend.post@it-university.nl

Question 2057

Which of the following types of attack often take advantage of curiosity or greed to deliver malware?

- ☒ Gimmes
- ☐ Tripwire
- ☐ Icing
- ☐ Soft coding
- ☐ Pretexting
- ☐ None of the choices.

Explanation:

Explanation:

Gimmes take advantage of curiosity or greed to deliver malware. Also known as a Trojan Horse, gimmes can arrive as an email attachment promising anything. The recipient is expected to give in to the need to the program and open the attachment. In addition, many users will blindly click on any attachments they receive that seem even mildly legitimate.

Question 2058

During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:

- ☐ event error log generated at the disaster recovery site.
- ☐ disaster recovery test plan.
- ☐ disaster recovery plan (DRP).
- ☒ configurations and alignment of the primary and disaster recovery sites.

Explanation:

Explanation:

Since the configuration of the system is the most probable cause, the IS auditor should review that first. If the issue cannot be clarified, the IS auditor should then review the event error log. The disaster recovery test plan and the disaster recovery plan (DRP) would not contain information about the system configuration.

Question 2059

Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

- ☐ Policies that require instant dismissal if such devices are found
- ☒ Software for tracking and managing USB storage devices
- ☐ Administratively disabling the USB port
- ☐ Searching personnel for USB storage devices at the facility's entrance

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissal may result in increased employee attrition and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching of personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

Question 2060

Which of the following step of PDCA establishes the objectives and processes necessary to deliver results in accordance with the expected output?

- ☒ Plan
- ☐ Do
- ☐ Check
- ☐ Act

Explanation:

Plan - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition."

The steps in each successive PDCA cycle are:

Licensed to Berend Post berend.post@it-university.nl

PLAN

Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

DO

Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

CHECK

Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

ACT

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

DO - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

CHECK - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences

ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

Question 2061

Which of the following virus prevention techniques can be implemented through hardware?

- ☒ Remote booting
- ☐ Heuristic scanners
- ☐ Behavior blockers
- ☐ Immunizers

Explanation:

Explanation:

Remote booting (e.g., diskless workstations) is a method of preventing viruses, and can be implemented through hardware. Choice C is a detection, not a prevention, although it is hardware-based. Choices B and D are not hard ware-based.

Question 2062

Which of the following is the MOST significant risk when an application uses individual end user accounts to access the underlying database?

- ☒ User accounts may remain active after a termination.
- ☐ Multiple connects to the database are used and slow the process.
- ☐ Application may not capture a complete audit trail.
- ☐ Users may be able to circumvent application controls.

Licensed to Berend Post berend.post@it-university.nl

Question 2063

Which of the following methods should be used to effectively erase sensitive data from portable storage devices that are to be reused?

- ☐ Formatting the portable device
- ☐ Using media sanitization software
- ☒ Overwriting the sensitive data
- ☐ Exposing the portable device to a magnetic field

Question 2064

Which of the following is MOST important for an organization to complete prior to developing its disaster recovery plan (DRP)?

- ☐ Support staff skill gap analysis
- ☐ Comprehensive IT inventory
- ☒ Business impact analysis (BIA)
- ☐ Risk assessment

Question 2065

How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

- ☒ EDI usually decreases the time necessary for review.
- ☐ EDI usually increases the time necessary for review.
- ☐ Cannot be determined.
- ☐ EDI does not affect the time necessary for review.

Explanation:

Explanation:

Electronic data interface (EDI) supports intervendor communication while decreasing the time necessary for review because it is usually configured to readily identify errors requiring follow-up.

Question 2066

Which of the following layer of an enterprise data flow architecture does the scheduling of the tasks necessary to build and maintain the Data Warehouse (DW) and also populates Data Marts?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☒ Warehouse management layer
- ☐ Data access layer

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Licensed to Berend Post berend.post@it-university.nl

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Licensed to Berend Post berend.post@it-university.nl

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Licensed to Berend Post berend.post@it-university.nl

Question 2067

Statistical sampling is NOT based on which of the following audit sample techniques?

- ☒ Haphazard Sampling
- ☐ Random Sampling
- ☐ Cell Sampling
- ☐ Fixed interval sampling

Explanation:

The NOT keyword is used in the question. You need find out an option which is NOT an example of statistical sampling. Statistical sampling is NOT based on Haphazard sampling.

For your exam you should know the information below

Audit samples are selected for the purpose of collecting representative evidence to be subjected to either compliance testing or substantive testing. The auditor should consider a selection technique that will provide the most relevant evidence supported by appropriate analytical procedures.

Two basic types of audit samples can be designed by the auditor to fulfill their requirements:

statistical and no statistical. Below Figure shows the various audit samples, as well as their testing methods. Care is given to the selection process in order to avoid drawing the wrong conclusion from the wrong sample. This is referred to as a sampling risk. Let's look at each of these samples more closely.

Statistical Sampling

Statistical sampling uses mathematical techniques that result in an outcome that is mathematically quantifiable. Statistical samples are usually presented as a percentage. The purpose of statistical sampling is to gain an objective representation. Samples are selected by an objective mathematical process. The auditor should be aware that if the client has strong internal controls, the sample sizes may be smaller because the odds of fraud or failure will be lower.

Examples of statistical sampling include the following:

Random sampling Samples are selected at random.

Cell sampling Random selection is performed at predefined intervals.

Fixed interval sampling The sample existing at every n + interval increment is selected for testing.

No statistical Sampling

No statistical sampling is based on the auditor's judgment (also referred to as judgmental sampling). The auditor determines the sample size, the method of generating the sample, and the number of

Licensed to Berend Post berend.post@it-university.nl

items to be analyzed. The results of judgmental sampling are unlikely to represent the actual population. This is a subjective process usually based on elements of risk or materiality. An example of no statistical sampling includes haphazard sampling, in which the samples are randomly drawn for testing.

After the samples are selected, the next step is to perform compliance tests or substantive testing.

Conducting Audit Testing As stated earlier, the basic test methods used will be either compliance testing or substantive testing. Appropriate audit samples will have to be generated for the test.

Compliance Testing

Compliance testing tests for the presence or absence of something. Compliance testing includes verifying that policies and procedures have been put in place, and checking that user access rights, program change control procedures, and system audit logs have been activated. An example of a compliance test is comparing the list of persons with physical access to the data center against the HR list of current employees.

Compliance testing is based on one of the following types of audit samples:

Attribute sampling Generally popular in compliance testing. The objective is to determine whether an attribute is present or absent in the subject sample. The result is specified by the rate of occurrence—for example, the presence of 1 in 100 units would be 1 percent.

Stop-and-go sampling Used when few errors are expected. Stop-and-go allows the test to occur without excessive effort in sampling and provides the opportunity to stop testing at the earliest possible opportunity. It is a simple form of testing to reinforce any claim that errors are unlikely in the sample population.

Discovery sampling A 100 percent sampling used to detect fraud or when the likelihood of evidence existing is low. Forensics is an excellent example of discovery sampling. This is an attempt to discover evidence.

Precision, or expected error rate The precision rate indicates the acceptable margin of error between audit samples and the total quantity of the subject population. This is usually expressed as a percentage, such as 5 percent. To obtain a very low error rate, it is necessary to use a very large sample in testing. Auditors are justified in using a smaller sample size when the total population is expected to be error-free. A larger sample is required when errors are expected to be present in the population. The larger sample can yield a higher average. When errors are expected, the auditor must examine more data to determine whether the actual errors are within a tolerable error rate (maximum errors you would accept).

Error levels may be determined by reviewing the findings of a prior audit and by considering changes in the organization's procedures. Use the risk-based audit strategy to determine whether your samples and tests are telling the truth about the audited.

Licensed to Berend Post berend.post@it-university.nl

Substantive Testing

Substantive testing seeks to verify the content and integrity of evidence. Substantive tests may include complex calculations to verify account balances, perform physical inventory counts, or execute sample transactions to verify the accuracy of supporting documentation. Substantive tests use audit samples selected by dollar value or to project (forecast or estimate) a total for groups with related characteristics.

Substantive testing is based on one of the following types of audit samples:

Variable sampling Used to designate dollar values or weights (effectiveness) of an entire subject population by prorating from a smaller sample. Consider the challenge of counting large volumes of currency by its weight. Variable sampling could be used to count currency by multiplying the physical weight of one unit by the total weight of the combined sample, and then multiplying by the face value printed on the bill or coin. A demonstration is a single $50 bill weighing 1.0 gram, with the entire sample of $50 bills weighing 61 grams altogether. The combined sample weight would indicate a total quantity of 61 bills for an estimated dollar value of $3,050. This is a common technique for forecasting quantity and value of inventory based on particular characteristics.

Unsatisfied mean estimation Used in an attempt to project an estimated total for the whole subject population.

Stratified mean estimation Used to calculate an average by group, similar to demographics, whereby the entire population is divided (stratified) into smaller groups based on similar characteristics.

Examples are teenagers from the ages of 13 to 19, people from the ages of 20 to 29, people from the ages of 30 to 39, and those who are male or female, smokers or nonsmokers, and so on. Difference estimation Used to determine the difference between audited and unaudited claims of value.

The following answers are incorrect:

The other options like Random Sampling, Cell Sampling and Fixed Interval Sampling are examples of Statistical sampling.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 55 to 56

CISA certified information system auditor study guide Second Edition Page Number 98 to 101

Licensed to Berend Post berend.post@it-university.nl

Question 2068

When a new system is to be implemented within a short time frame, it is MOST important to:

- ☐ finish writing user manuals.
- ☒ perform user acceptance testing.
- ☐ add last-minute enhancements to functionalities.
- ☐ ensure that the code has been documented and reviewed.

Explanation:

Explanation:

It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirement.

Question 2069

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- ☐ Diskless workstations
- ☐ Data encryption techniques
- ☒ Network monitoring devices
- ☐ Authentication systems

Explanation:

Explanation:

Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations prevent access control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environment wide, logical facilities that can differentiate among users, before providing access to systems.

Licensed to Berend Post berend.post@it-university.nl

Question 2070

Overall business risk for a particular threat can be expressed as:

- ☒ a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
- ☐ the magnitude of the impact should a threat source successfully exploit the vulnerability.
- ☐ the likelihood of a given threat source exploiting a given vulnerability.
- ☐ the collective judgment of the risk assessment team.

Explanation:

Explanation:

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

Question 2071

A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon. The MOST effective plan of action would be to:

- ☒ use analytical tools to produce exception reports from the system and performance monitoring software
- ☐ re-install the system and performance monitoring software
- ☐ evaluate replacement systems and performance monitoring software
- ☐ restrict functionality of system monitoring software to security-related events

Question 2072

An IS auditor observes that an organization's critical IT systems have experienced several failures throughout the year. Which of the following is the BEST recommendation?

- ☐ Perform a disaster recovery test.
- ☒ Perform a root cause analysis.
- ☐ Contract for a hot site.
- ☐ Implement redundant systems.

Licensed to Berend Post berend.post@it-university.nl

Question 2073

Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

- ☐ Call forwarding
- ☒ Privacy release
- ☐ Tenanting
- ☐ Voice mail

Explanation:

Privacy release supports shared extensions among several devices, ensuring that only one device at a time can use an extension.

For your exam you should know below mentioned PBX features and Risks:

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking

Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)

Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Licensed to Berend Post berend.post@it-university.nl

Fraud, user tracking, non authorized features

Access Codes

Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features

Silent Monitoring

Silently monitors other calls

Eavesdropping

Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference

override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping

Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting

Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Licensed to Berend Post berend.post@it-university.nl

Illegal usage, fraud, eavesdropping

Voice mail

Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Privacy release

Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics

Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting

When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Licensed to Berend Post berend.post@it-university.nl

Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting -Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number358

Question 2074

During a disaster recovery audit, an IS auditor finds that a business impact analysis (BIA) has not been performed. The auditor should FIRST:

- ☐ perform a business impact analysis (BIA).
- ☐ issue an intermediate report to management.
- ☒ evaluate the impact on current disaster recovery capability.
- ☐ ?onduct additional compliance testing.

Licensed to Berend Post berend.post@it-university.nl

Question 2075

Which of the following is MOST important to include in a contract with a software development service provider?

- ☐ A list of key performance indicators (KPIs)
- ☒ Ownership of intellectual property
- ☐ Service level agreement (SLA)
- ☐ Explicit contract termination requirements

Question 2076

Which of the following is the BEST way for an information security manager to justify continued investment in the information security program when the organization is facing significant budget cuts?

- ☐ Demonstrate an increase in ransomware attacks targeting peer organizations.
- ☐ Demonstrate the readiness of business continuity plans.
- ☐ Demonstrate that implemented program controls are effective.
- ☒ Demonstrate that the program enables business activities.

Question 2077

When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

- ☒ they are set to meet security and performance requirements.
- ☐ changes are recorded in an audit trail and periodically reviewed.
- ☐ changes are authorized and supported by appropriate documents.
- ☐ access to parameters in the system is restricted.

Explanation:

Explanation:

The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing them is a detective control; however, if parameters are not set according to business rules, monitoring of changes may not be an effective control. Reviewing changes to ensure they are supported by appropriate documents is also a detective control, if parameters are set incorrectly, the related documentation and the fact that these are authorized does not reduce the impact. Restriction of access to parameters ensures that only authorized staff can access the parameters; however, if the parameters are set incorrectly, restricting access will still have an adverse impact.

Licensed to Berend Post berend.post@it-university.nl

Question 2078

Which of the following is MOST important for an IS auditor to consider when reviewing the effectiveness of an incident response program?

- ☐ Incidents are categorized according to industry standards.
- ☒ Lessons learned are incorporated into incident response processes.
- ☐ Incidents are escalated to senior management in a timely manner.
- ☐ The plan is reviewed and updated annually.

Question 2079

As part of a follow-up of a previous year's audit, an IS auditor has increased the expected error rate for a sample. The impact will be:

- ☐ degree of assurance increases.
- ☐ standard deviation decreases.
- ☐ sampling risk decreases.
- ☒ required sample size increases.

Question 2080

A source code repository should be designed to:

- ☐ provide automatic incorporation and distribution of modified code.
- ☒ prevent changes from being incorporated into existing code.
- ☐ provide secure versioning and backup capabilities for existing code.
- ☐ prevent developers from accessing secure source code.

Question 2081

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- ☒ compromises the Wireless Application Protocol (WAP) gateway.
- ☐ installs a sniffing program in front of the server.
- ☐ steals a customer's PDA.
- ☐ listens to the wireless transmission.

Explanation:

Explanation:

In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised, all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

Licensed to Berend Post berend.post@it-university.nl

Question 2082

Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

- ☐ restricted to predefined MAC addresses.
- ☐ encrypted using static keys.
- ☒ encrypted using dynamic keys.
- ☐ initiated from devices that have encrypted storage.

Explanation:

Explanation:

When using dynamic keys, the encryption key is changed frequently, thus reducing the risk of the key being compromised and the message being decrypted. Limiting the number of devices that can access the network does not address the issue of encrypting the session. Encryption with static keys-using the same key for a long period of time-risks that the key would be compromised. Encryption of the data on the connected device (laptop, PDA, etc.) addresses the confidentiality of the data on the device, not the wireless session.

Question 2083

Which of the following type of lock uses a numeric keypad or dial to gain entry?

- ☐ Bolting door locks
- ☒ Cipher lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Explanation:

The combination door lock or cipher lock uses a numeric key pad, push button, or dial to gain entry, it is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

A cipher lock, is controlled by a mechanical key pad, typically 5 to 10 digits that when pushed in the right combination the lock will releases and allows entry. The drawback is someone looking over a shoulder can see the combination. However, an electric version of the cipher lock is in production in which a display screen will automatically move the numbers around, so if someone is trying to watch the movement on the screen they will not be able to identify the number indicated unless they are standing directly behind the victim.

Remember locking devices are only as good as the wall or door that they are mounted in and if the frame of the door or the door itself can be easily destroyed then the lock will not be effective. A lock will eventually be defeated and its primary purpose is to delay the attacker.

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below types of lock

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique physical attribute such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

The following were incorrect answers:

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 376

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25144-25150). Acerbic Publications. Kindle Edition.

Licensed to Berend Post berend.post@it-university.nl

Question 2084

An organization using instant messaging to communicate with customers can prevent legitimate customers from being impersonated by:

- ☐ using call monitoring.
- ☐ using firewalls to limit network traffic to authorized ports.
- ☐ logging conversations.
- ☒ authenticating users before conversations are initiated.

Question 2085

In a botnet, mailbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

- ☒ Chat system
- ☐ SMS system
- ☐ Email system
- ☐ Log system
- ☐ Kernel system
- ☐ None of the choices.

Explanation:

Explanation:

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware or mailbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

Question 2086

As part of business continuity planning, which of the following is MOST important to include in a business impact analysis (BIA)?

- ☐ Define a risk appetite.
- ☐ Assess risk of moving significant applications to the cloud.
- ☐ Assess recovery scenarios.
- ☒ Assess threats to the organization.

Licensed to Berend Post berend.post@it-university.nl

Question 2087

Many WEP systems require a key in a relatively insecure format. What format is this?

- ☐ binary format.
- ☒ hexadecimal format.
- ☐ 128 bit format.
- ☐ 256 bit format.
- ☐ None of the choices.

Explanation:

Explanation:

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

Many WEP systems require a key in hexadecimal format. If one chooses keys that spell words in the limited 0-9, A-F hex character set, these keys can be easily guessed.

Question 2088

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- ☐ Dumping the memory content to a file
- ☐ Generating disk images of the compromised system
- ☒ Rebooting the system
- ☐ Removing the system from the network

Explanation:

Explanation:

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

Question 2089

Which of the following types of attack almost always requires physical access to the targets?

- ☒ Direct access attack
- ☐ Wireless attack
- ☐ Port attack
- ☐ Window attack
- ☐ System attack
- ☐ None of the choices.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Direct access attacks make use of common consumer devices that can be used to transfer data surreptitiously. Someone gaining physical access to a computer can install all manner of devices to compromise security, including operating system modifications, software worms, keyboard loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

Question 2090

During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

- ☒ Identification
- ☐ Data integrity
- ☐ Data validation
- ☐ Authentication

Question 2091

Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?

- ☐ datagram scanning
- ☒ access lists
- ☐ stateful inspection
- ☐ state checking
- ☐ link progressing
- ☐ None of the choices.

Explanation:

Explanation:

In addition to deploying stateful firewall, you may setup basic traffic filtering on a more sophisticated router. As an example, on a Cisco IOS based router you may use ip access lists (ACL) to perform basic filtering on the network edge. Note that if they have denied too much traffic, something is obviously being too restrictive and you may want to reconfigure them.

Question 2092

What can be used to gather evidence of network attacks?

- ☐ Access control lists (ACL)
- ☒ Intrusion-detection systems (IDS)
- ☐ Syslog reporting
- ☐ Antivirus programs

Explanation:

Explanation:

Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

Licensed to Berend Post berend.post@it-university.nl

Question 2093

To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

- ☒ Secure Shell (SSH-2) tunnel for the duration of the problem.
- ☐ two-factor authentication mechanism for network access.
- ☐ dial-in access.
- ☐ virtual private network (VPN) account for the duration of the vendor support contract.

Explanation:

Explanation:

For granting temporary access to the network, a Secure Shell (SSH-2) tunnel is the best approach. It has auditing features and allows restriction to specific access points. Choices B, C and D all give full access to the internal network. Two-factor authentication and virtual private network (VPN) provide access to the entire network and are suitable for dedicated users. Dial-in access would need to be closely monitored or reinforced with another mechanism to ensure authentication to achieve the same level of security as SSH-2.

Question 2094

Which of the following controls will MOST effectively detect inconsistent records resulting from the lack of referential integrity in a database management system?

- ☒ Concurrent access controls
- ☐ Incremental data backups
- ☐ Performance monitoring tools
- ☐ Periodic table link checks

Question 2095

Which of the following is the BEST way to detect software license violations?

- ☐ Implementing a corporate policy on copyright infringements and software use.
- ☐ Requiring that all PCs be diskless workstations.
- ☐ Installing metering software on the LAN so applications can be accessed through the metered software.
- ☒ Regularly scanning PCs in use to ensure that unauthorized copies of software have not been loaded on the PC.

Explanation:

The best way to prevent and detect software license violations is to regularly scan used PCs, either from the LAN or directly, to ensure that unauthorized copies of software have not been loaded on the PC.

Licensed to Berend Post berend.post@it-university.nl

Other options are not detective.

A corporate policy is not necessarily enforced and followed by all employees.

Software can be installed from other means than floppies or CD-ROMs (from a LAN or even downloaded from the Internet) and software metering only concerns applications that are registered.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 108).

Question 2096

An IS auditor seeks assurance that a new process for purging transactions does not have a detrimental impact on the integrity of a database. This could be achieved BEST by analyzing the:

- ☐ database structure.
- ☐ design of triggers.
- ☐ results of the process in a test environment.
- ☒ entity relationship diagram of the database.

Question 2097

Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

- ☐ Parallel testing
- ☐ Pilot testing
- ☐ Interface/integration testing
- ☒ Sociability testing

Explanation:

Explanation:

The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system- and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective is to take unit-tested modules and build an integrated structure.

 Licensed to Berend Post berend.post@it-university.nl

Question 2098

Which of the following threats is prevented by using token-based authentication?

- ☒ Password sniffing attack on the network
- ☐ Session eavesdropping attack on the network
- ☐ Man-in-the-middle attack on the client
- ☐ Denial of service attack over the network

Question 2099

Sam is the security Manager of a financial institute. Senior management has requested he performs a risk analysis on all critical vulnerabilities reported by an IS auditor. After completing the risk analysis, Sam has observed that for a few of the risks, the cost benefit analysis shows that risk mitigation cost (countermeasures, controls, or safeguard) is more than the potential lost that could be incurred. What kind of a strategy should Sam recommend to the senior management to treat these risks?

- ☐ Risk Mitigation
- ☒ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Explanation:

Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

For your exam you should know below information about risk assessment and treatment:

A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. A risk assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security controls, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows

management the amount of resources that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

Identify assets and their value to the organization.

Identify vulnerabilities and threats.

Licensed to Berend Post berend.post@it-university.nl

Quantify the probability and business impact of these potential threats.

Provide an economic balance between the impact of the threat and the cost

of the countermeasure.

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance.

It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before committing to owning, insuring, and driving a motor vehicle.

Licensed to Berend Post berend.post@it-university.nl

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if, indeed, the company has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could have a catastrophic effect on the company's ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase of new hardware, software, and office equipment, while transference of the risk to an insurance company would require premium payments. The

executive then further notes that minimal impact to the organization would occur if any of the reported low-level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to forgo the costs and accept the risk. In the young driver example, risk acceptance could be based on the observation that the youngster has demonstrated the responsibility and maturity to warrant the parent's trust in his or her judgment.

The following answers are incorrect:

Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

Risk Avoidance - Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized.

Risk Mitigation -Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 51

and

Official ISC2 guide to CISSP CBK 3rd edition page number 534-539

Question 2100

Which of the following component of an expert system allows the expert to enter knowledge into the system without the traditional mediation of a software engineer?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☒ Knowledge interface

Explanation:

Knowledge interface allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

For CISA Exam you should know below information about Artificial Intelligence and Expert System

Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used

Goals are generated and achieved

Information is communicated

Collaboration is achieved

Concepts are formed

Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.

Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface

 Licensed to Berend Post berend.post@it-university.nl

with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degrees Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

Knowledge interface – Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule - Expressing declarative knowledge through the use of if-then relationships.

Semantic nets - Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 187

Question 2101

Which of the following methods should be used to purge confidential data from write-once optical media?

- ☐ Degauss the media.
- ☒ Destroy the media.
- ☐ Remove the references to data from the access index.
- ☐ Write over the data with null values.

Question 2102

Human error is being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☐ DDoS
- ☐ ATP
- ☒ Social Engineering
- ☐ None of the choices.

Question 2103

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- ☐ Discussion with management
- ☐ Review of the organization chart
- ☒ Observation and interviews
- ☐ Testing of user access rights

Explanation:

Explanation: By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

Licensed to Berend Post berend.post@it-university.nl

Question 2104

In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

- ☐ application programmer copy the source program and compiled object module to the production libraries
- ☐ application programmer copy the source program to the production libraries and then have the production control group compile the program.
- ☐ production control group compile the object module to the production libraries using the source program in the test environment.
- ☒ production control group copy the source program to the production libraries and then compile the program.

Explanation:

Explanation:

The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

Question 2105

An organization is considering using production data for testing a new application's functionality. Which of the following data protection techniques would BEST ensure that personal data cannot be inadvertently recovered in test environments while also reducing the need for strict confidentiality of the data?

- ☒ Data anonymization
- ☐ Data minimization
- ☐ Data normalization
- ☐ Data encryption

Question 2106

Which of the following BEST enables staff acceptance of information security policies?

- ☒ Strong senior management support
- ☐ Adequate security funding
- ☐ Computer-based training
- ☐ A robust incident response program

Licensed to Berend Post berend.post@it-university.nl

Question 2107

Which of the following would BEST assist an information security manager in gaining strategic support from executive management?

- ☐ Research on trends in global information security breaches
- ☒ Risk analysis specific to the organization
- ☐ Annual report of security incidents within the organization
- ☐ Rating of the organization's security based on international standards

Question 2108

An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are in place. The BEST response the auditor can make is to:

- ☐ review the integrity of system access controls.
- ☐ accept management's statement that effective access controls are in place.
- ☒ stress the importance of having a system control framework in place.
- ☐ review the background checks of the accounts payable staff.

Explanation:

Explanation:

Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

Question 2109

The FIRST step in data classification is to:

- ☒ establish ownership.
- ☐ perform a criticality analysis.
- ☐ define access rules.
- ☐ create a data dictionary.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Data classification is necessary to define access rules based on a need-to-do and need-to- know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for protection of data, which takes input from data classification. Access definition is complete after data classification and input for a data dictionary is prepared from the data classification process.

Question 2110

What would be an IS auditor's BEST recommendation upon finding that a third-party IT service provider hosts the organization's human resources (HR) system in a foreign country?

- ☒ Conduct a privacy impact analysis.
- ☐ Implement change management review.
- ☐ Review third-party audit reports.
- ☐ Perform background verification checks.

Question 2111

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

Question 2112

There are several types of penetration tests depending upon the scope, objective and nature of a test. Which of the following describes a penetration test where you attack and attempt to circumvent the controls of the targeted network from the outside, usually the Internet?

- ☒ External Testing
- ☐ Internal Testing
- ☐ Blind Testing
- ☐ Targeted Testing

Explanation:

External testing refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system, usually the Internet.

For the CISA exam you should know penetration test types listed below:

Licensed to Berend Post berend.post@it-university.nl

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system, usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Double Blind Testing -It is an extension of blind testing, since the administrator and security staff at the target are also not aware of test. Such a testing can effectively evaluate the incident handling and response capability of the target and how well managed the environment is.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

The following were incorrect answers:

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such a testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

Licensed to Berend Post berend.post@it-university.nl

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 369

Question 2113

A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the BESTcourse of action to address the situation?

- ☐ Require that new systems that can meet the standards be implemented.
- ☐ Document the deficiencies in the risk register.
- ☒ Develop processes to compensate for the deficiencies.
- ☐ Disconnect the legacy system from the rest of the network.

Question 2114

An IS auditor finds that the process for removing access for terminated employees is not documented. What is the MOST significant risk from this observation?

- ☐ Procedures may not align with best practices.
- ☐ HR records may not match system access.
- ☐ Unauthorized access cannot be identified.
- ☒ Access rights may not be removed in a timely manner.

Question 2115

Which of the following would BEST demonstrate that an effective disaster recovery plan (DRP) is in place?

- ☐ Periodic risk assessment
- ☒ Full operational test
- ☐ Frequent testing of backups
- ☐ Annual walk-through testing

Question 2116

An IS auditor reviewing the threat assessment for a data center would be MOST concerned if:

- ☐ all identified threats relate to external entities
- ☐ some of the identified threats are unlikely to occur
- ☐ neighboring organizations' operations have been included
- ☒ the exercise was completed by local management

Licensed to Berend Post berend.post@it-university.nl

Question 2117

Which of the following statement INCORRECTLY describes the Control self-assessment (CSA) approach?

- ☒ CSA is policy or rule driven
- ☐ CSA Empowered/accountable employees
- ☐ CSA focuses on continuous improvement/learning curve
- ☐ In CSA, Staffs at all level, in all functions, are the primary control analyst.

Explanation:

Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out an option which incorrectly describes Control Self-assessment.

For your exam you should know the information below about control self-assessment:

Control self-assessment is an assessment of controls made by the staff and management of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal controls of the organization are reliable.

Benefits of CSA

Early detection of risk

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives

Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

Highly motivated employees

Improved audit training process

Reduction in control cost

Assurance provided to stakeholders and customers

Traditional and CSA attributes

Licensed to Berend Post berend.post@it-university.nl

Traditional Historical CSA

Assign duties/supervises staff Empowered/accountable employees

Policy/rule driven Continuous improvement/learning curve

Limited employee participation Extensive employee participation and training

Narrow stakeholders focus Broad stakeholders focus

Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are correctly describes about CSA.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 61, 62 and 63

Question 2118

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager would be to:

- ☐ review the state of security awareness
- ☐ perform a gap analysis
- ☒ perform a risk assessment
- ☐ review information security policies

Question 2119

Identify the INCORRECT statement related to network performance below?

- ☐ Bandwidth - Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred
- ☒ Latency - Latency the actual rate that information is transferred
- ☐ Jitter - Jitter variation in the time of arrival at the receiver of the information
- ☐ Error Rate - Error rate the number of corrupted bits expressed as a percentage or fraction of the total sent

Explanation:

The word INCORRECT is the keyword used within the question. You need to find out a statement which is incorrectly describe about network performance. Throughput the actual rate that information is transferred and Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

 Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sent

The following answers are incorrect:

The other options correctly describe network performance parameters.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 275

Question 2120

When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

- ☐ node list.
- ☐ acceptance test report.
- ☒ network diagram.
- ☐ user's list.

Explanation:

Explanation:

To properly review a LAN implementation, an IS auditor should first verify the network diagram and confirm the approval. Verification of nodes from the node list and the network diagram would be next, followed by a review of the acceptance test report and then the user's list.

Question 2121

Which of the following statement is NOT true about Voice-Over IP (VoIP)?

- ☒ VoIP uses circuit switching technology
- ☐ Lower cost per call or even free calls, especially for long distance call
- ☐ Lower infrastructure cost
- ☐ VoIP is a technology where voice traffic is carried on top of existing data infrastructure

Explanation:

The NOT is a keyword used in the question. You need to find out invalid statement about VoIP. VoIP uses packet switching and not circuit switching.

For your exam you should know below information about VoIP:

Voice-Over-IP

IP telephony, internet telephony, is the technology that makes it possible to have a voice conversation over the Internet or over any dedicated IP network instead of dedicated transmission lines. The protocol is used to carry the signal over the IP network are commonly referred as Voice-Over-IP (VoIP).VoIP is a technology where voice traffic is carried on top of existing data infrastructure. Sounds are digitalized into IP packets and transferred through the network layer before being decode back into the original voice.

Licensed to Berend Post berend.post@it-university.nl

VoIP allows the elimination of circuit switching and the associated waste of bandwidth. Instead, packet switching is used, where IP packets with voice data are sent over the network only when data needs to be sent.

It has advantages over traditional telephony:

Unlike traditional telephony, VoIP innovation progresses at market rates rather than at the rates of multilateral committee process of the International Telecommunication Union (ITU)

Lower cost per call or even free calls, especially for long distance call

Lower infrastructure costs. Once IP infrastructure is installed, no or little additional telephony infrastructure is needed

VoIP Security Issues

With the introduction of VoIP, the need for security is more important because it is needed to protect two assets – the data and the voice.

Protecting the security of conversation is vital now.

In VoIP, packets are sent over the network from the user's computer or VoIP phone to similar equipment at other end. Packets may pass through several intermediate systems that are not under the control of the user's ISP.The current Internet architecture does not provide same physical wire security as phone line.

The main concern of VoIP solution is that while, in the case of traditional telephones, if data system is disrupted, then the different sites of the organization could still be reached via telephone. Thus a backup communication facility should be planned for if the availability of communication is vital to organization.

Another issue might arise with the fact that IP telephones and their supporting equipment require the same care and maintenance as computer system do.

To enhance the protection of the telephone system and data traffic, the VoIP infrastructure should be segregated using Virtual Local Area Network (VLAN).

In many cases, session border controllers (SBCs) are utilized to provide security features for VoIP traffic similar to that provided by firewalls.

The following were incorrect answers:

 Licensed to Berend Post berend.post@it-university.nl

Lower cost per call or even free calls, especially for long distance call - This is a valid statement about VoIP. In fact it is an advantage of VoIP.

Lower infrastructure cost - This is a valid statement and advantage of using VoIP as compare to traditional telephony system.

VoIP is a technology where voice traffic is carried on top of existing data infrastructure – This is also valid statement about VoIP.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number355

Question 2122

Which of the following should an IS auditor be MOST concerned with when a system uses radio frequency identification (RFID)?

- ☐ Scalability
- ☐ Maintainability
- ☒ Nonrepudiation
- ☐ Privacy

Question 2123

The MAIN criterion for determining the severity level of a service disruption incident is:

- ☐ cost of recovery.
- ☐ negative public opinion.
- ☐ geographic location.
- ☒ downtime.

Explanation:

Explanation:

The longer the period of time a client cannot be serviced, the greater the severity of the incident. The cost of recovery could be minimal yet the service downtime could have a major impact.

Negative public opinion is a symptom of an incident. Geographic location does not determine the severity of the incident.

Licensed to Berend Post berend.post@it-university.nl

Question 2124

When auditing a software development project, a review of which of the following will BEST verify that project work is adequately subdivided?

- ☒ Work breakdown structure
- ☐ Statement of work
- ☐ Scope statement
- ☐ Functional and technical design documents

Question 2125

A hacker could obtain passwords without the use of computer tools or programs through the technique of:

- ☒ social engineering.
- ☐ sniffers.
- ☐ back doors.
- ☐ Trojan horses.

Explanation:

Explanation:

Social engineering is based on the divulgence of private information through dialogues, interviews, inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal data. A sniffer is a computer tool to monitor the traffic in networks. Back doors are computer programs left by hackers to exploit vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually malicious in nature.

Question 2126

Which of the following provides an IS auditor the MOST assurance that an organization is compliant with legal and regulatory requirements?

- ☐ The IT manager is responsible for the organization's compliance with legal and regulatory requirements.
- ☒ Controls associated with legal and regulatory requirements have been identified and tested.
- ☐ Senior management has provided attestation of legal and regulatory compliance.
- ☐ There is no history of complaints or fines from regulators regarding noncompliance.

Licensed to Berend Post berend.post@it-university.nl

Question 2127

Which of the following should be of GREATEST concern to an IS auditor reviewing an organization's information security program?

- ☐ The program was not formally signed off by the sponsor.
- ☒ Key performance indicators (KPIs) are not established.
- ☐ Not all IT staff are aware of the program.
- ☐ The program was last updated five years ago.

Question 2128

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

- ☐ variable sampling.
- ☐ substantive testing.
- ☒ compliance testing.
- ☐ stop-or-go sampling.

Explanation:

Explanation:

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing; such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

Question 2129

A disaster recovery plan for an organization should:

- ☒ reduce the length of the recovery time and the cost of recovery.
- ☐ increase the length of the recovery time and the cost of recovery.
- ☐ reduce the duration of the recovery time and increase the cost of recovery.
- ☐ affect neither the recovery time nor the cost of recovery.

Explanation:

Explanation:

One of the objectives of a disaster recovery plan is to reduce the duration and cost of recovering from a disaster. A disaster recovery plan would increase the cost of operations before and after the disaster occurs, but should reduce the time to return to normal operations and the cost that could result from a disaster.

Licensed to Berend Post berend.post@it-university.nl

Question 2130

Which of the following BEST restricts users to those functions needed to perform their duties?

- ☒ Application level access control
- ☐ Data encryption
- ☐ Disabling floppy disk drives
- ☐ Network monitoring device

Explanation:

Explanation:

The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

Question 2131

Which of the following physical access controls effectively reduces the risk of piggybacking?

- ☐ Biometric door locks
- ☐ Combination door locks
- ☒ Deadman doors
- ☐ Bolting door locks

Explanation:

Explanation:

Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding areA. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint or signature activate biometric door locks; however, they do not prevent or reduce the risk of piggybacking. Combination door locks, also known as cipher locks, use a numeric key pad or dial to gain entry. They do not prevent or reduce the risk of piggybacking since unauthorized individuals may still gain access to the processing center. Bolting door locks require the traditional metal key to gain entry. Unauthorized individuals could still gain access to the processing center along with an authorized individual.

Question 2132

When developing a business continuity plan (BCP), business unit management's involvement is MOST important during the:

- ☐ performance of a business impact analysis (BIA).
- ☒ development of business recovery procedures.
- ☐ implementation of a document repository.
- ☐ performance of an IT risk assessment.

Licensed to Berend Post berend.post@it-university.nl

Question 2133

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

Question 2134

Which of the following are valid choices for the Apache/SSL combination (Choose three.):

- ☒ the Apache-SSL project
- ☒ third-party SSL patches
- ☒ the mod_ssl module
- ☐ the mod_css module
- ☐ None of the choices.

Explanation:

Explanation:

On Linux you have Apache which is supposed to be a safer choice of web service. In fact you have several choices for the Apache/SSL combination, such as the Apache-SSL project (www.apache-ssl.org) using third-party SSL patches, or have Apache compiled with the mod_ssl module.

Question 2135

An organization's IT security policy requires annual security awareness training for all employees. Which of the following would provide the BEST evidence of the training's effectiveness?

- ☒ Results of a social engineering test
- ☐ Interviews with employees
- ☐ Decreased calls to the incident response team
- ☐ Surveys completed by randomly selected employees

Licensed to Berend Post berend.post@it-university.nl

Question 2136

An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

- ☐ check to ensure that the type of transaction is valid for the card type.
- ☒ verify the format of the number entered then locate it on the database.
- ☐ ensure that the transaction entered is within the cardholder's credit limit.
- ☐ confirm that the card is not shown as lost or stolen on the master file.

Explanation:

Explanation:

The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in place. Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

Question 2137

Following an unauthorized disclosure of data, an organization needs to implement data loss prevention (DLP) measures. The IS auditor's BEST recommendation should be to:

- ☐ install DLP software on corporate servers to prevent recurrence.
- ☐ monitor and block outgoing emails based on common DLP criteria.
- ☐ restrict removable media access on all computer systems.
- ☒ establish a risk and control framework.

Question 2138

Responsibility for the governance of IT should rest with the:

- ☐ IT strategy committee.
- ☐ chief information officer (CIO).
- ☐ audit committee.
- ☒ board of directors.

Explanation:

Explanation:

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

Licensed to Berend Post berend.post@it-university.nl

Question 2139

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

- ☐ Observe the response mechanism.
- ☐ Clear the virus from the network.
- ☒ Inform appropriate personnel immediately.
- ☐ Ensure deletion of the virus.

Explanation:

Explanation:

The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response. Choice A should be taken after choice

C. This will enable an IS auditor to examine the actual workability and effectiveness of the response system. An IS auditor should not make changes to the system being audited, and ensuring the deletion of the virus is a management responsibility.

Question 2140

The PRIMARY purpose of a precedence diagramming method in managing IT projects is to:

- ☐ monitor project scope creep.
- ☒ identify the critical path.
- ☐ identify key milestones.
- ☐ minimize delays and overruns.

Question 2141

Which audit technique provides the GREATEST assurance that incident management procedures are effective?

- ☐ Determining whether incidents are categorized and addressed
- ☒ Performing comprehensive vulnerability scanning and penetration testing
- ☐ Comparing incident management procedures to best practices
- ☐ Evaluating end-user satisfaction survey results

Licensed to Berend Post berend.post@it-university.nl

Question 2142

A firewall has been installed on the company's web server. Which concern does the firewall address?

- ☐ Availability of the information
- ☐ Unauthorized modification of information by internal users
- ☒ Accessing information by the outside world
- ☐ Connectivity to the Internet

Question 2143

Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

- ☐ Router
- ☒ Bridge
- ☐ Repeater
- ☐ Gateway

Explanation:

Explanation:

A bridge connects two separate networks to form a logical network (e.g., joining an Ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet.

Question 2144

An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

- ☒ Denial-of-service
- ☐ Replay
- ☐ Social engineering
- ☐ Buffer overflow

Explanation:

Explanation:

Prior to launching a denial-of-service attack, hackers often use automatic port scanning software to acquire information about the subject of their attack. A replay attack is simply sending the same packet again. Social engineering exploits end-user vulnerabilities, and buffer overflow attacks exploit poorly written code.

Licensed to Berend Post berend.post@it-university.nl

Question 2145

An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

- ☐ The corporate network is using an intrusion prevention system (IPS)
- ☒ This part of the network is isolated from the corporate network
- ☐ A single sign-on has been implemented in the corporate network
- ☐ Antivirus software is in place to protect the corporate network

Explanation:

Explanation:

If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or being physically separated. An I PS would detect possible attacks, but only after they have occurred. A single sign-on would ease authentication management. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

Question 2146

IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

- ☐ Inadequate screen/report design facilities
- ☐ Complex programming language subsets
- ☐ Lack of portability across operating systems
- ☒ Inability to perform data intensive operations

Explanation:

Explanation:

4GLs are usually not suitable for data intensive operations. Instead, they are used mainly for graphic user interface (GUI) design or as simple query/report generators.

Question 2147

An IS auditor discovers instances where software with the same license key is deployed to multiple workstations, in breach of the licensing agreement. Which of the following is the auditor's BEST recommendation?

- ☐ Evaluate the business case for funding of additional licenses.
- ☐ Require business owner approval before granting software access.
- ☐ Remove embedded keys from offending packages.
- ☒ Implement software licensing monitoring to manage duplications.

Licensed to Berend Post berend.post@it-university.nl

Question 2148

Which of the following property of the core date warehouse layer of an enterprise data flow architecture uses common attributes to access a cross section of an information in the warehouse?

- ☐ Drill up
- ☐ Drill down
- ☒ Drill across
- ☐ Historical Analysis

Explanation:

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Licensed to Berend Post berend.post@it-university.nl

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Licensed to Berend Post berend.post@it-university.nl

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 2149

After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?

- ☒ Balanced scorecard
- ☐ Recent audit results
- ☐ Risk heat map
- ☐ Gap analysis

Question 2150

Which of the following is a substantive test procedure?

- ☒ Using audit software to verify the total of an accounts receivable file
- ☐ Observing that user IDs and passwords are required to sign on to the online system
- ☐ Test of invoice calculation process
- ☐ Verifying that appropriate approvals are documented in a sample of program changes

Question 2151

An IS auditor performing detailed network assessments and access control reviews should FIRST:

- ☒ determine the points of entry.
- ☐ evaluate users' access authorization.
- ☐ assess users' identification and authorization.
- ☐ evaluate the domain-controlling server configuration.

Explanation:

Explanation:

In performing detailed network assessments and access control reviews, an IS auditor should first determine the points of entry to the system and review the points of entry accordingly for appropriate controls. Evaluation of user access authorization, assessment of user identification and authorization, and evaluation of the domain-controlling server configuration are all implementation issues for appropriate controls for the points of entry.

Licensed to Berend Post berend.post@it-university.nl

Question 2152

When performing a data classification project, an information security manager should:

- ☒ assign information critically and sensitivity
- ☐ identify information owners
- ☐ identify information custodians
- ☐ assign information access privileges

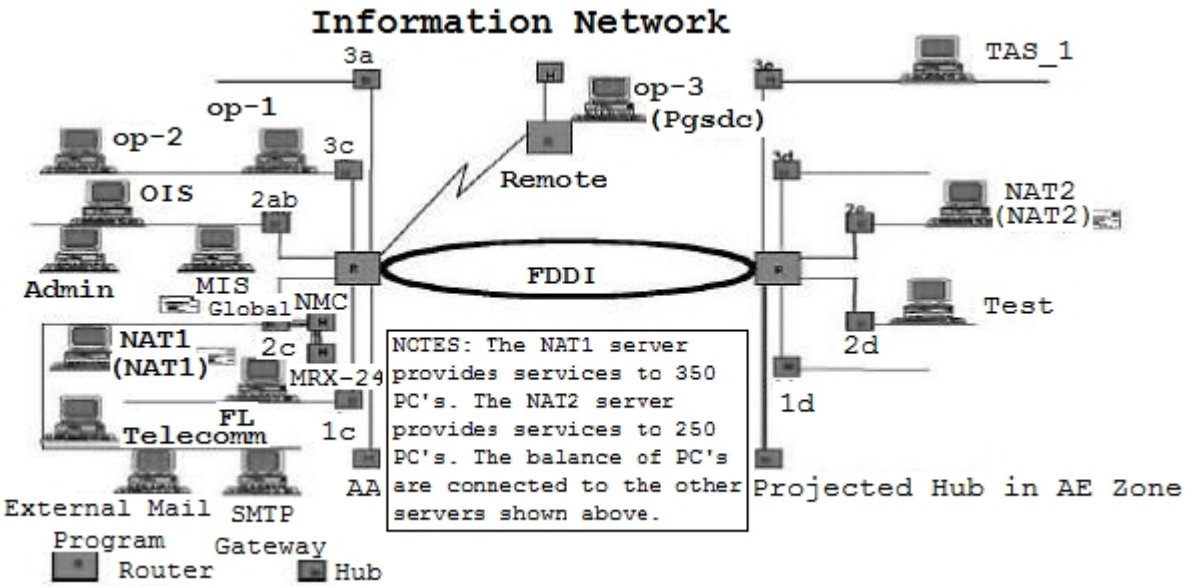
Question 2153

Which of the following will enable a customer to authenticate an online Internet vendor?

- ☐ Vendor signs a reply using a hash function and the customer's public key.
- ☐ Customer encrypts an order using the vendor's public key.
- ☒ Customer verifies the vendor's certificate with a certificate authority (CA).
- ☐ Vendor decrypts incoming orders using its own private key.

Question 2154

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



- ☐ No firewalls are needed
- ☐ Op-3 location only
- ☐ MIS (Global) and NAT2
- ☒ SMTP Gateway and op-3

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The objective of a firewall is to protect a trusted network from an untrusted network; therefore, locations needing firewall implementations would be at the existence of the external connections. All other answers are incomplete or represent internal connections.

Question 2155

Which of the following transmission media is LEAST vulnerable to cross talk?

- ☐ Copper cable
- ☒ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Explanation:

Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Licensed to Berend Post berend.post@it-university.nl

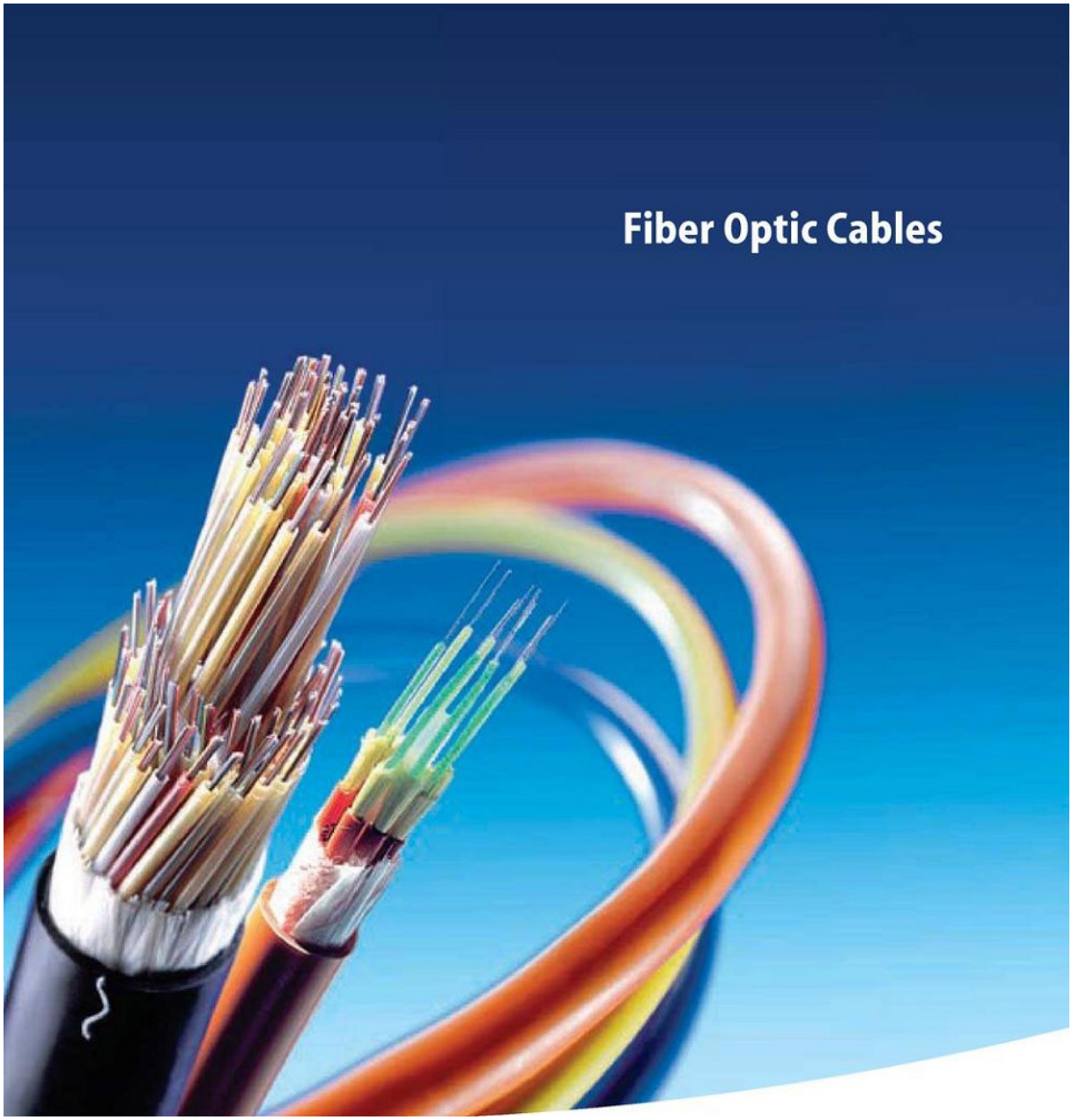
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

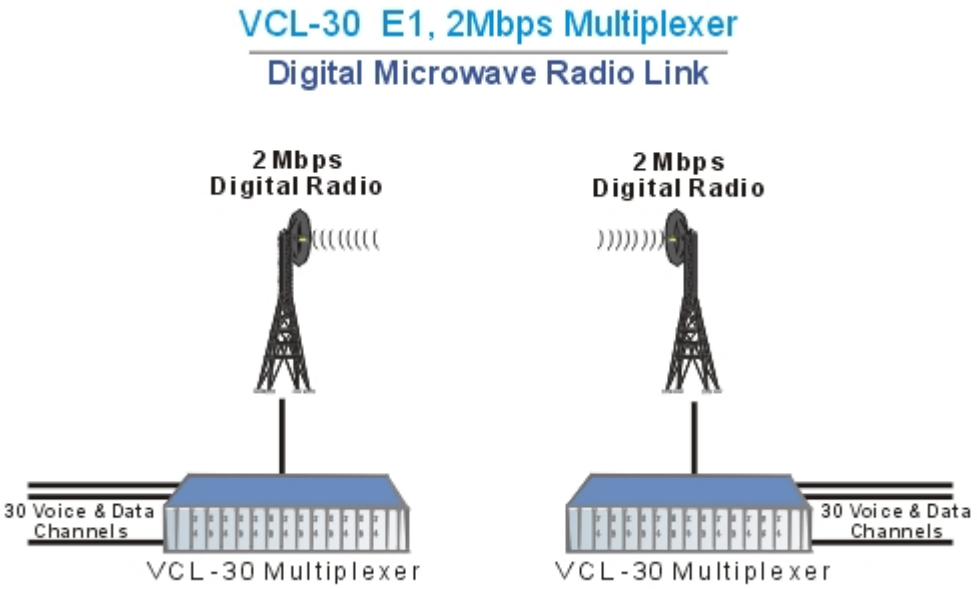
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Licensed to Berend Post berend.post@it-university.nl

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System

Radio systems are used for short distance, cheap and easy to tap.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Licensed to Berend Post berend.post@it-university.nl

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Coaxial cable - Coaxial cable are expensive and does not support many LAN's. It supports data and video

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

Question 2156

When using an integrated test facility (ITF), an IS auditor should ensure that:

- ☐ production data are used for testing.
- ☒ test data are isolated from production data.
- ☐ a test data generator is used.
- ☐ master files are updated with the test data.

Explanation:

Explanation:

An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production data. An IS auditor is not required to use production data or a test data generator. Production master files should not be updated with test data.

Licensed to Berend Post berend.post@it-university.nl

Question 2157

During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

- ☒ Storage area network (SAN)
- ☐ Network Attached Storage (NAS)
- ☐ Network file system (NFS v2)
- ☐ Common Internet File System (CIFS)

Explanation:

Explanation:

In contrast to the other options, in a SAN comprised of computers, FC switches or routers and storage devices, there is no computer system hosting and exporting its mounted file system for remote access, aside from special file systems. Access to information stored on the storage devices in a SAN is comparable to direct attached storage, which means that each block of data on a disk can be addressed directly, since the volumes of the storage device are handled as though they are local, thus providing optimal performance. The other options describe technologies in which a computer (or appliance) shares its information with other systems. To access the information, the complete file has to be read.

Question 2158

During the system testing phase of an application development project the IS auditor should review the:

- ☐ conceptual design specifications.
- ☐ vendor contract.
- ☒ error reports.
- ☐ program change requests.

Explanation:

Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

Licensed to Berend Post berend.post@it-university.nl

Question 2159

Which of the following BEST helps to identify errors during data transfer?

- ☐ Decrease the size of data transfer packets.
- ☒ Test the integrity of the data transfer.
- ☐ Review and verify the data transfer sequence numbers.
- ☐ Enable a logging process for data transfer.

Question 2160

An organization's IT security policy states that user IDs must uniquely identify individuals and that users should not disclose their passwords. An IS auditor discovers that several generic user IDs are being used. Which of the following is the MOST appropriate course of action for the auditor?

- ☒ Investigate the noncompliance.
- ☐ Include the finding in the final audit report.
- ☐ Recommend disciplinary action.
- ☐ Recommend a change in security policy.

Question 2161

An organization's business continuity plan should be:

- ☒ updated based on changes to personnel and environments.
- ☐ updated only after independent audit review by a third party.
- ☐ tested whenever new applications are implemented.
- ☐ tested after successful intrusions into the organization's hot site.

Question 2162

While reviewing the business continuity plan of an organization, an IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

- ☐ Deterrence
- ☒ Mitigation
- ☐ Recovery
- ☐ Response

Explanation:

Explanation:

An effective business continuity plan includes steps to mitigate the effects of a disaster. Files must be restored on a timely basis for a backup plan to be effective. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organization's hot site to restore normal business operations.

Licensed to Berend Post berend.post@it-university.nl

Question 2163

Which of the following is NOT an example of preventive control?

- ☐ Physical access control like locks and door
- ☐ User login screen which allows only authorize user to access website
- ☒ Encrypt the data so that only authorize user can view the same
- ☐ Duplicate checking of a calculations

Explanation:

Explanation:

The word NOT is used as a keyword in the question. You need to find out a security control from given options which in not preventive. Duplicate checking of a calculation is a detective control and not a preventive control.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Licensed to Berend Post berend.post@it-university.nl

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to

find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other

technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective

nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Licensed to Berend Post berend.post@it-university.nl

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security

incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take

many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

 Licensed to Berend Post berend.post@it-university.nl

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Licensed to Berend Post berend.post@it-university.nl

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Licensed to Berend Post berend.post@it-university.nl

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples belong to Preventive control.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 2164

_____ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance.

- ☐ Data custodians
- ☒ The board of directors and executive officers
- ☐ IT security administration
- ☐ Business unit managers

Explanation:

Explanation:

The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

Question 2165

Which of the following would BEST help ensure information security is effective following the outsourcing of network operations?

- ☐ Test security controls periodically.
- ☐ Review security key performance indicators (KPIs).
- ☒ Establish security service level agreements (SLAs).
- ☐ Appoint a security service delivery monitoring manager.

Licensed to Berend Post berend.post@it-university.nl

Question 2166

Reconciliations have identified data discrepancies between an enterprise data warehouse and a revenue system for key financial reports. What is the GREATEST risk to the organization in this situation?

- ☐ The key financial reports may no longer be produced
- ☐ Financial reports may be delayed
- ☒ Undetected fraud may occur
- ☐ Decisions may be made based on incorrect information

Question 2167

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

- ☐ Minimizing costs for the services provided
- ☐ Prohibiting the provider from subcontracting services
- ☐ Evaluating the process for transferring knowledge to the IT department
- ☒ Determining if the services were provided as contracted

Explanation:

Explanation:

From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department.

Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

Question 2168

A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the BEST way to obtain assurance that the provider can adequately protect the organization's information?

- ☐ Check references supplied by the provider's other customers.
- ☒ Invoke the right to audit per the contract.
- ☐ Review the provider's information security policy.
- ☐ Review the provider's self-assessment.

Licensed to Berend Post berend.post@it-university.nl

Question 2169

Which of the following type of a computer network covers a limited area such as a home, office or campus?

- ☒ LAN
- ☐ WAN
- ☐ SAN
- ☐ PAN

Explanation:

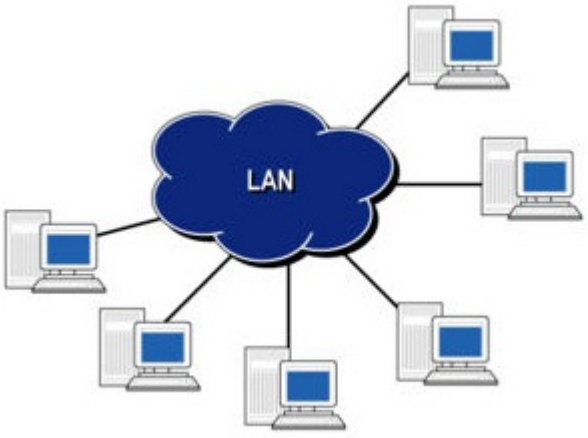
A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

Local Area Network

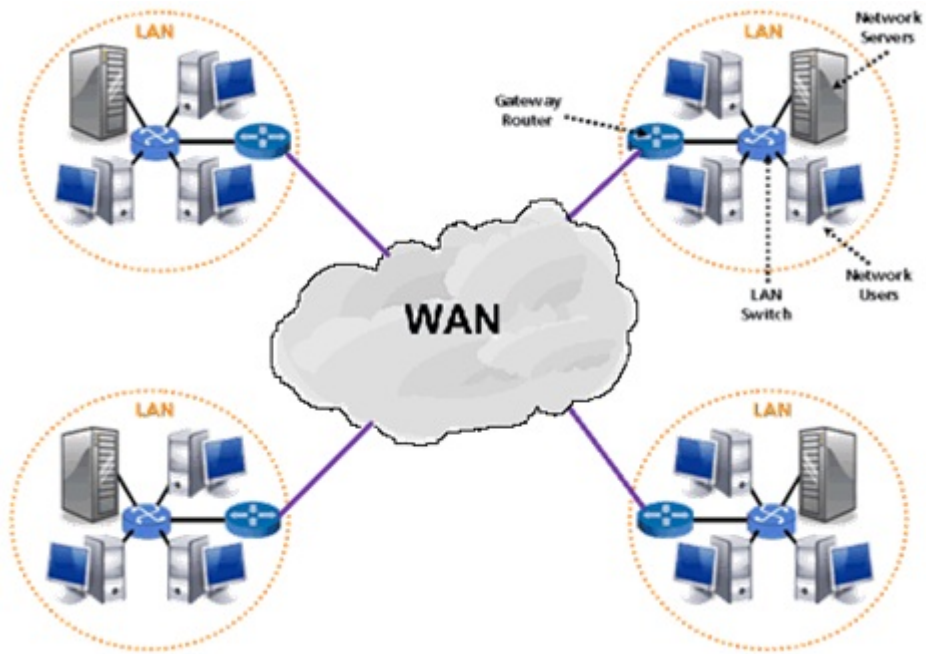


Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Licensed to Berend Post berend.post@it-university.nl

Wide Area Network

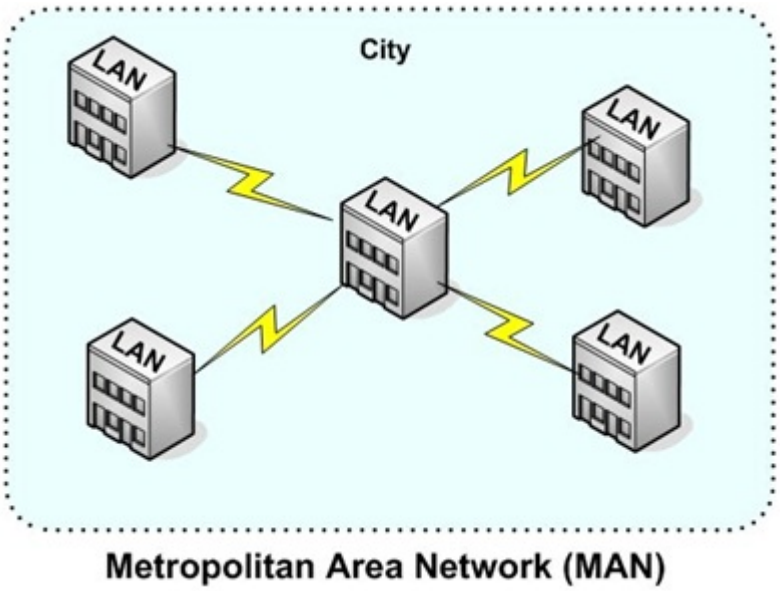


Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

Licensed to Berend Post berend.post@it-university.nl

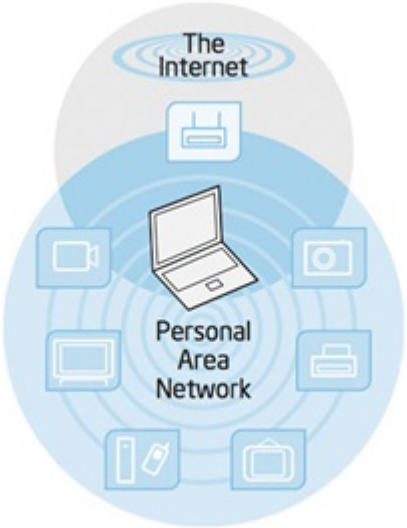


Metropolitan Area Network (MAN)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to

Licensed to Berend Post berend.post@it-university.nl

the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

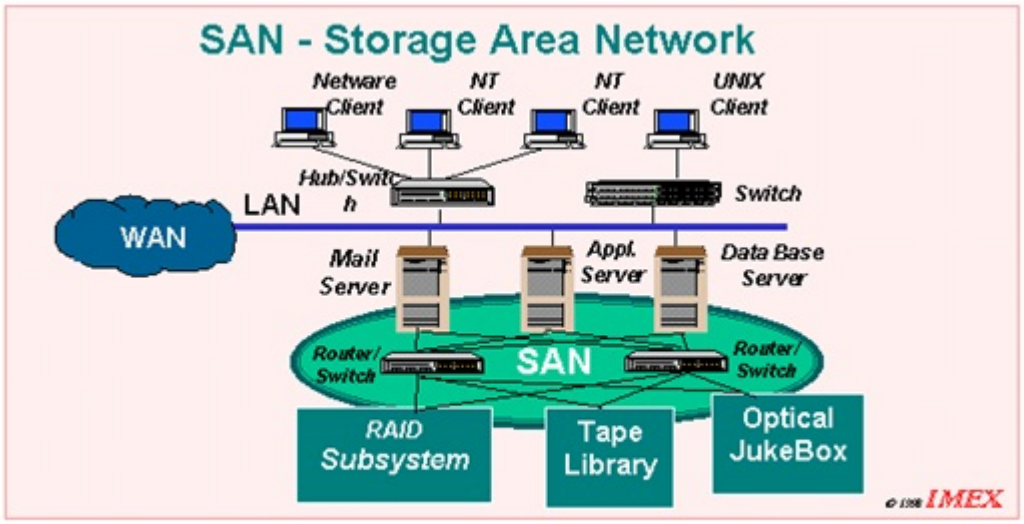


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

WAN - A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

SAN - A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 258

Licensed to Berend Post berend.post@it-university.nl

Question 2170

A web organization is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

- ☐ Code review by a third party
- ☐ Web application firewall implementation
- ☒ Penetration test results
- ☐ Database application monitoring logs

Question 2171

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic badge system for access to a data center?

- ☒ Increasing accountability
- ☐ Maintaining compliance
- ☐ Tracking employee work hours
- ☐ Increasing reliability

Question 2172

A change to the scope of an IT project has been formally submitted to the project manager. What should the project manager do NEXT?

- ☐ Update the project plan to reflect the change in scope
- ☒ Discuss the change with the project team and determine if it should be approved
- ☐ Escalate the change to the change advisory board for approval
- ☐ Determine how the change will affect the schedule and budget

Question 2173

Which of the following would be best suited to oversee the development of an information security policy?

- ☐ System Administrators
- ☐ End User
- ☒ Security Officers
- ☐ Security administrators

Explanation:

The security officer would be the best person to oversee the development of such policies.

Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end users. Policies that are poorly written, or written at too high of an

Licensed to Berend Post berend.post@it-university.nl

education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.

Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is expected of them and the consequences of noncompliance can come down to a liability issue.

While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the business issues are addressed.

The security officers will get better corporate support by including other areas in policy development. This helps build buy-in by these areas as they take on a greater ownership of the final product. Consider including areas such as HR, legal, compliance, various IT areas and specific business area representatives who represent critical business units.

When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations. Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility. Such placement of these documents plus checklists, forms, and sample documents can make awareness more effective.

For your exam you should know the information below:

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Executive Management/Senior Management -Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know.

Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are

 Licensed to Berend Post berend.post@it-university.nl

responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines.

Information Systems Security Professional-Drafting of security policies, standards and supporting guidelines, procedures, and baselines is coordinated through these individuals. Guidance is provided for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed in this role.

Data/Information/Business/System Owners - A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.

Data/Information Custodian/Steward - A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed, by systems administrators. This group administers access rights to the information assets.

Information Systems Auditor-IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Business Continuity Planner -Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery.

Licensed to Berend Post berend.post@it-university.nl

Information Systems/ Technology Professionals-These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Network/Systems Administrator - A systems administrator (sysadmin /netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

Physical Security - The individuals assigned to the physical security role establish relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigation (FBI) to assist in investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of the closed circuit television (CCTV) surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, and legal and business areas to ensure that the practices are integrated.

Security Analyst - The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines. Whereas the previous roles are “in the weeds” and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level.

Licensed to Berend Post berend.post@it-university.nl

Administrative Assistants/Secretaries - This role can be very important to information security; in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on the goodwill of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or of providing unauthorized entry.

Help Desk Administrator - As the name implies, the help desk is there to field questions from users that report system problems. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk is also often where the first indications of security issues and incidents will be seen. A help desk individual would contact the computer security incident response team (CIRT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.

Supervisor - The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees' account information is up-to-date; and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

Change Control Analyst Since the only thing that is constant is change, someone must make sure changes happen securely. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens.

The following answers are incorrect:

Systems Administrator - A systems administrator (sysadmin/ netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability

 Licensed to Berend Post berend.post@it-university.nl

management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 109

Harris, Shun (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw-Hill. Kindle Edition.

Question 2174

A policy has been established requiring users to install mobile device management (MDM) software on their personal devices. Which of the following would BEST mitigate the risk created by noncompliance with this policy?

- ☐ Issuing warnings and documenting noncompliance
- ☒ Disabling remote access from the mobile device
- ☐ Issuing company-configured mobile devices
- ☐ Requiring users to sign-off on terms and conditions

Question 2175

When removing a financial application system from production, which of the following is MOST important?

- ☐ Media used by the retired system has been sanitized.
- ☒ Data retained for regulatory purposes can be retrieved.
- ☐ End-user requests for changes are recorded and tracked.
- ☐ Software license agreements are retained.

Licensed to Berend Post berend.post@it-university.nl

Question 2176

A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- ☒ what amount of progress against schedule has been achieved.
- ☐ if the project budget can be reduced.
- ☐ if the project could be brought in ahead of schedule.
- ☐ if the budget savings can be applied to increase the project scope.

Explanation:

Explanation:

Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position, it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget after adjusting for actual progress, this is not necessarily a good outcome because it points to flaws in the original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may be the wrong thing to do.

Question 2177

Which of the following would an IS auditor consider to be the MOST significant risk associated with a project to reengineer a business process?

- ☐ The negative impact of change may not be documented.
- ☐ The project manager is inexperienced in information systems.
- ☒ Existing controls may be weakened or removed.
- ☐ Existing baseline processes may not be reported to management.

Licensed to Berend Post berend.post@it-university.nl

Question 2178

Which of the following is BEST enabled by following a configuration management process for new applications?

- ☐ Deploying approved emergency changes to production
- ☐ Ensuring proper testing of code before deployment
- ☐ Managing successful implementation of acquired software
- ☒ Maintaining adequate control over changes to production

Question 2179

An external security audit risk has reported multiple instances of control noncompliance. Which of the following would be MOSTimportant for the information security manager to communicate to senior management?

- ☒ The impact of noncompliance on the organization's risk profile
- ☐ An accountability report to initiate remediation activities
- ☐ A plan for mitigating the risk due to noncompliance
- ☐ Control owner responses based on a root cause analysis

Question 2180

Which of the following is MOST important for an IS auditor to verify when reviewing an organization's information security practices following the adoption of a bring your own device (BYOD) program?

- ☐ Only applications approved by information security may be installed on devices.
- ☐ The expected benefits of adopting the BYOD program have been realized.
- ☒ Security policies have been updated to include BYOD.
- ☐ Remote wipe is enabled for devices allowed by BYOD.

Question 2181

Which of the following would create the GREATEST risk when migrating a critical legacy system to a new system?

- ☐ Using agile development methodology
- ☐ Following a phased approach
- ☒ Following a direct cut-over approach
- ☐ Maintaining parallel systems

Licensed to Berend Post berend.post@it-university.nl

Question 2182

Which of the following findings should be of MOST concern to an IS auditor when evaluating information security governance within an organization?

- ☐ The data center manager has final sign-off on security projects.
- ☐ The information security oversight committee meets quarterly.
- ☒ The information security department has difficulty filling vacancies.
- ☐ Information security policies were last updated two years ago.

Question 2183

What is the PRIMARY purpose of audit trails?

- ☐ To document auditing efforts
- ☐ To correct data integrity errors
- ☒ To establish accountability and responsibility for processed transactions
- ☐ To prevent unauthorized access to data

Explanation:

Explanation:

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

Question 2184

Which of the following would be the GREATEST concern to an IS auditor reviewing a critical spreadsheet during a financial audit?

- ☐ Periodic access reviews are manually performed.
- ☒ Changes to the file are not always documented.
- ☐ Access requests are manually processed.
- ☐ A copy current validated file is not available.

Question 2185

Which of the following actions should an organization's security policy require an employee to take upon finding a security breach?

- ☒ Report the incident to the manager immediately.
- ☐ Inform IS audit management immediately.
- ☐ Confirm the breach can be exploited.
- ☐ Devise appropriate countermeasures.

Licensed to Berend Post berend.post@it-university.nl

Question 2186

What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

- ☐ Document existing internal controls
- ☐ Perform compliance testing on internal controls
- ☐ Establish a controls-monitoring steering committee
- ☒ Identify high-risk areas within the organization

Explanation:

Explanation:

When implementing continuous-monitoring systems, an IS auditor's first step is to identify high-risk areas within the organization.

Question 2187

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

- ☐ registration authority (RA).
- ☒ certificate authority (CA).
- ☐ certificate repository.
- ☐ receiver.

Explanation:

Explanation:

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

Question 2188

Which of the following refers to the proving of mathematical theorems by a computer program?

- ☐ Analytical theorem proving
- ☐ Automated technology proving
- ☐ Automated theorem processing
- ☒ Automated theorem proving
- ☐ None of the choices.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Automated theorem proving (ATP) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification.

Question 2189

What would an IS auditor expect to find in the console log?

- ☐ Evidence of password spoofing
- ☒ System errors
- ☐ Evidence of data copy activities
- ☐ Evidence of password sharing

Explanation:

Explanation:

An IS auditor can expect to find system errors to be detailed in the console log.

Question 2190

The most common reason for the failure of information systems to meet the needs of users is that:

- ☐ user needs are constantly changing.
- ☐ the growth of user requirements was forecast inaccurately.
- ☐ the hardware system limits the number of concurrent users.
- ☒ user participation in defining the system's requirements was inadequate.

Explanation:

Explanation:

Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are, and therefore what the system should accomplish.

Question 2191

What is a primary high-level goal for an auditor who is reviewing a system development project?

- ☐ To ensure that programming and processing environments are segregated
- ☐ To ensure that proper approval for the project has been obtained
- ☒ To ensure that business objectives are achieved
- ☐ To ensure that projects are monitored and administrated effectively

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A primary high-level goal for an auditor who is reviewing a systems- development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

Question 2192

An organization plans to deploy Wi-Fi location analytics to count the number of shoppers per day across its various retail outlets. What should the IS auditor recommend as the FIRST course of action by IT management?

- ☒ Conduct a privacy impact assessment
- ☐ Mask media access control (MAC) addresses
- ☐ Survey shoppers for feedback
- ☐ Develop a privacy notice to be displayed to shoppers

Question 2193

Which of the following should be of GREATEST concern to an IS auditor reviewing the controls for a continuous software release process?

- ☐ Release documentation is not updated to reflect successful deployment.
- ☐ Test libraries have not been reviewed in over six months.
- ☒ Developers are able to approve their own releases.
- ☐ Testing documentation is not attached to production releases.

Question 2194

Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?

- ☐ Redundant controls may be implemented across divisions
- ☐ Information security governance could be decentralized by divisions
- ☒ Areas of highest risk may not be adequately prioritized for treatment
- ☐ Return on investment may be inconsistently reported to senior management

Question 2195

The GREATEST benefit in implementing an expert system is the:

- ☒ capturing of the knowledge and experience of individuals in an organization.
- ☐ sharing of knowledge in a central repository.
- ☐ enhancement of personnel productivity and performance.
- ☐ reduction of employee turnover in key departments.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit; however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

Question 2196

During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?

- ☐ A biometric, digitalized and encrypted parameter with the customer's public key
- ☒ A hash of the data that is transmitted and encrypted with the customer's private key
- ☐ A hash of the data that is transmitted and encrypted with the customer's public key
- ☐ The customer's scanned signature encrypted with the customer's public key

Explanation:

Explanation:The calculation of a hash, or digest, of the data that are transmitted and its encryption require the public key of the client (receiver) and is called a signature of the message, or digital signature.

The receiver performs the same process and then compares the received hash, once it has been decrypted with their private key, to the hash that is calculated with the received data. If they are the same, the conclusion would be that there is integrity in the data that have arrived and the origin is authenticated. The concept of encrypting the hash with the private key of the originator provides non repudiation, as it can only be decrypted with their public key and, as the CD suggests, the private key would not be known to the recipient. Simply put, in a key-pair situation, anything that can be decrypted by a sender's public key must have been encrypted with their private key, so they must have been the sender, i.e., non-repudiation. Choice C is incorrect because, if this were the case, the hash could not be decrypted by the recipient, so the benefit of non-repudiation would be lost and there could be no verification that the message had not been intercepted and amended. A digital signature is created by encrypting with a private key. A person creating the signature uses their own private key, otherwise everyone would be able to create a signature with any public key. Therefore, the signature of the client is created with the client's private key, and this can be verified—by the enterprise—using the client's public key. Choice B is the correct answer because, in this case, the customer uses their private key to sign the hash data.

Licensed to Berend Post berend.post@it-university.nl

Question 2197

If the inherent risk of a business activity is higher than the acceptable risk level, the information security manager should FIRST:

- ☐ transfer risk to a third party to avoid cost of impact
- ☐ implement controls to mitigate the risk to an acceptable level
- ☐ recommend that management avoids the business activity
- ☒ assess the gap between current and acceptable level of risk

Question 2198

Which of the following is the FIRST step when conducting a business impact analysis?

- ☒ Identifying critical information resources
- ☐ Identifying events impacting continuity of operations
- ☐ Analyzing past transaction volumes
- ☐ Creating a data classification scheme

Question 2199

Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?

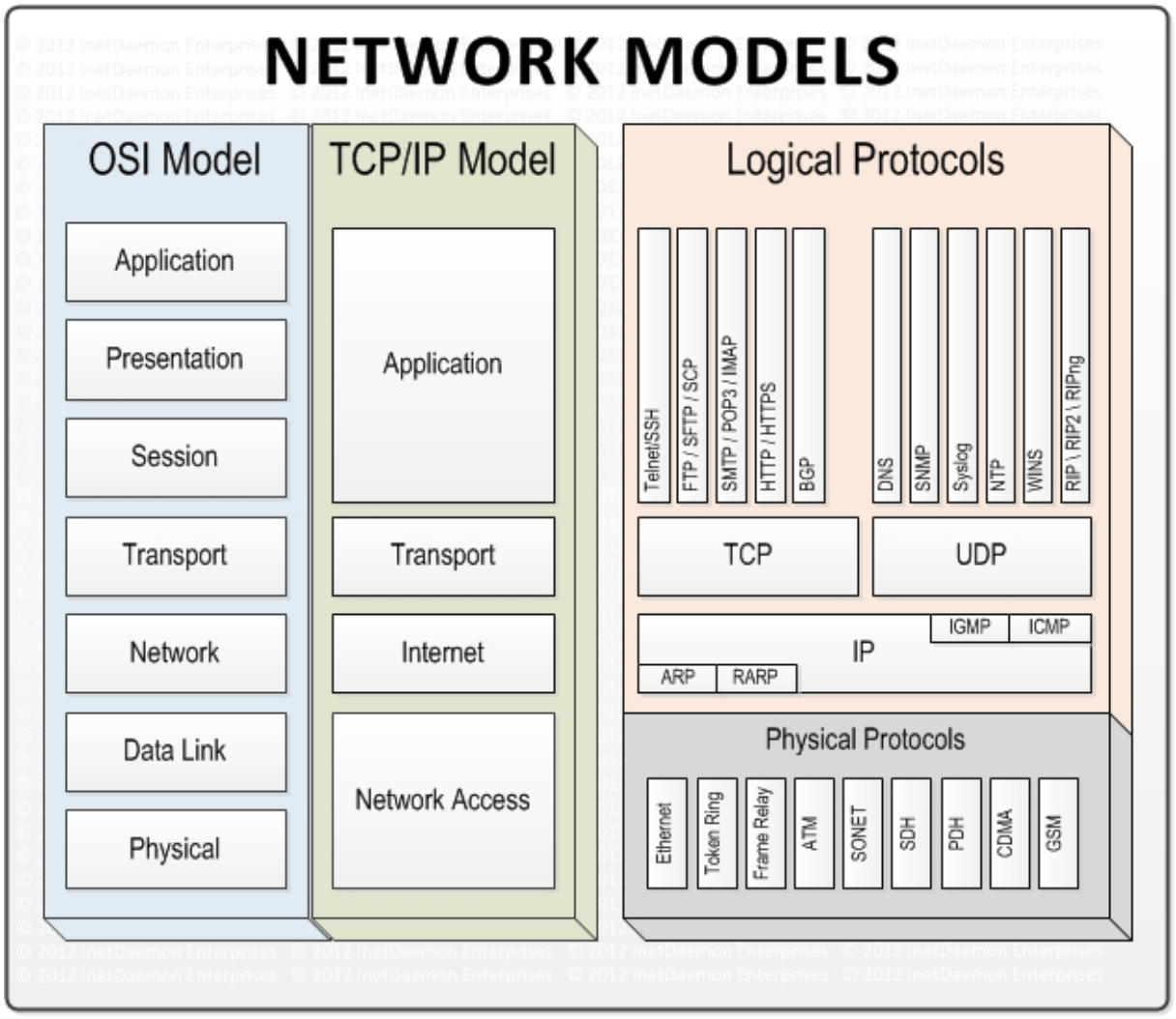
- ☐ Data
- ☐ Segment
- ☐ Packet
- ☒ Frame and bits

Explanation:

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

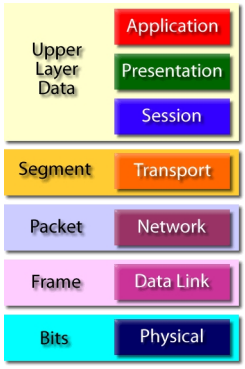
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

Data – Application layer data PDU

Segment – Transport layer data PDU

Packet – Network interface layer data PDU

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Question 2200

Which of the following activities is MOST important to consider when conducting IS audit planning?

- ☐ Results from previous audits are reviewed.
- ☐ Audit scheduling is based on skill set of audit team.
- ☒ Resources are allocated to areas of high risk.
- ☐ The audit committee agrees on risk rankings.

Licensed to Berend Post berend.post@it-university.nl

Question 2201

An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- ☒ this lack of knowledge may lead to unintentional disclosure of sensitive information.
- ☐ information security is not critical to all functions.
- ☐ IS audit should provide security training to the employees.
- ☐ the audit finding will cause management to provide continuous training to staff.

Explanation:

Explanation:

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

Question 2202

When auditing the IT governance of an organization planning to outsource a critical financial application to a cloud vendor, the MOST important consideration for the auditor should be:

- ☐ the cost of the outsourced system.
- ☐ the inclusion of a service termination clause.
- ☐ alignment with industry standards.
- ☒ alignment with business requirements.

Question 2203

Which of the following device in Frame Relay WAN technique is generally customer owned device that provides a connectivity between company's own network and the frame relays network?

- ☒ DTE
- ☐ DCE
- ☐ DME
- ☐ DLE

Explanation:

Data Terminal Equipment (DTE) - Usually a customer owned device that provides connectivity between company's own network and the frame relay's network.

For your exam you should know below information about WAN Technologies:

Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your

 Licensed to Berend Post berend.post@it-university.nl

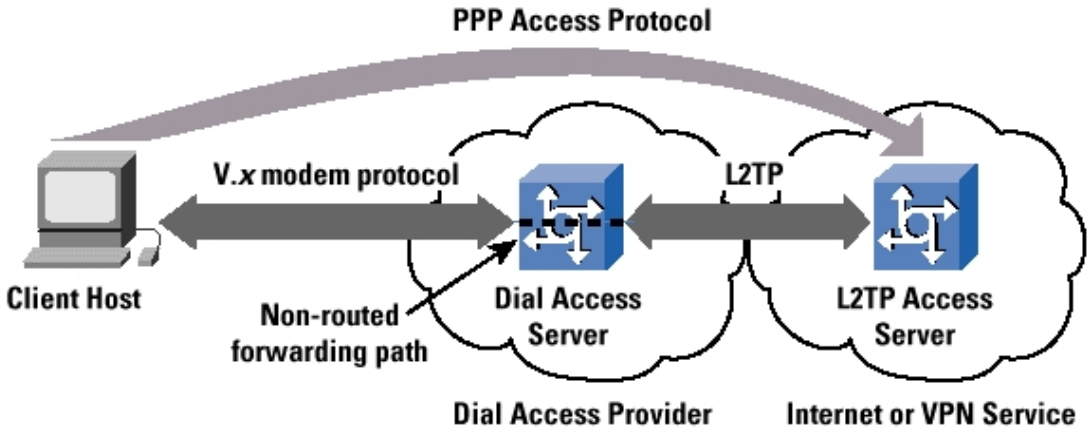
Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you.

PPP uses the Internet protocol (IP) (and is designed to handle other protocol as well). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Point-to-point protocol



X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

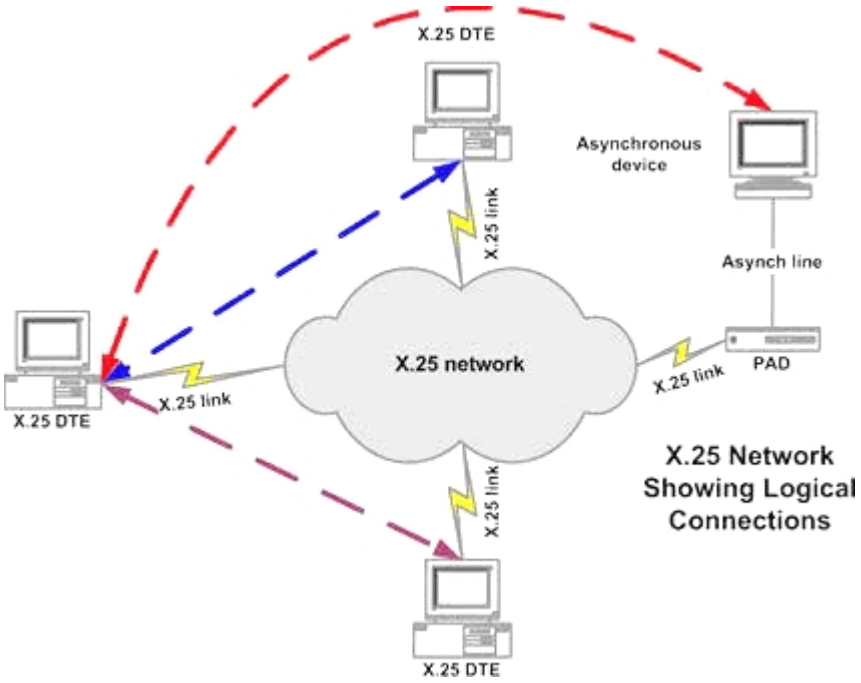
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Licensed to Berend Post berend.post@it-university.nl

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

X.25



Frame Relay

Works as packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Two main types of equipment's are used in Frame Relay

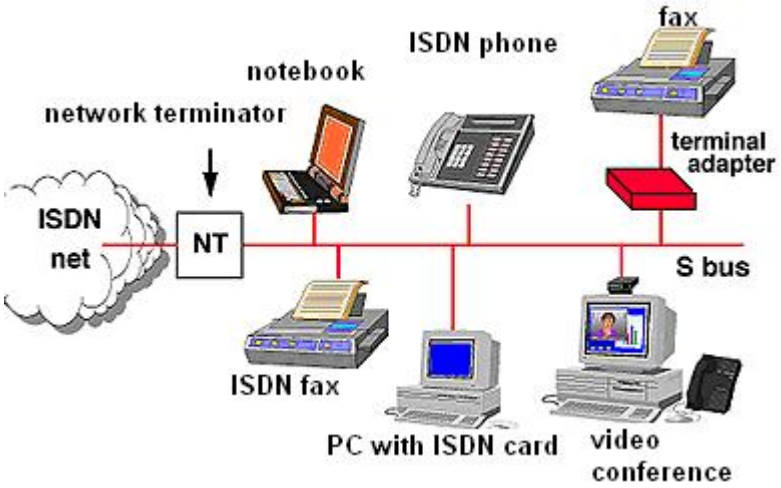
1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides connectivity between company's own network and the frame relay's network.

Licensed to Berend Post berend.post@it-university.nl

2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

Frame Relay



Integrated Service Digital Network (ISDN)

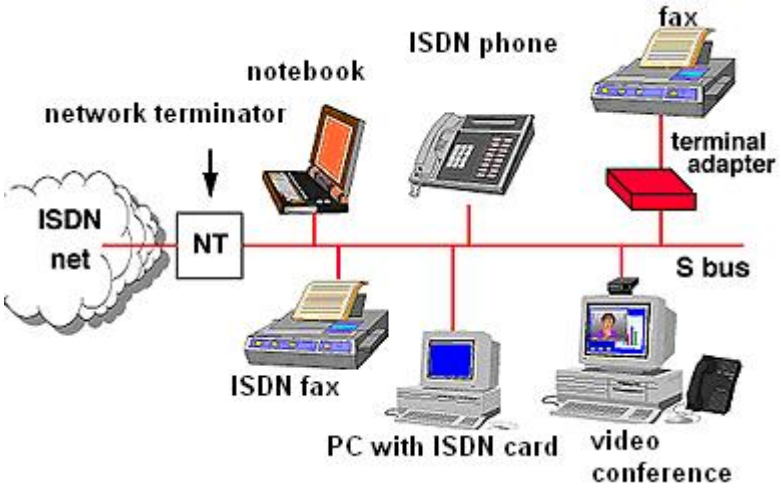
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Runs on top of the Plain Old Telephone System (POTS). The same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.

ISDN

Licensed to Berend Post berend.post@it-university.nl



Asynchronous Transfer Mode (ATM)

Uses Cell switching method

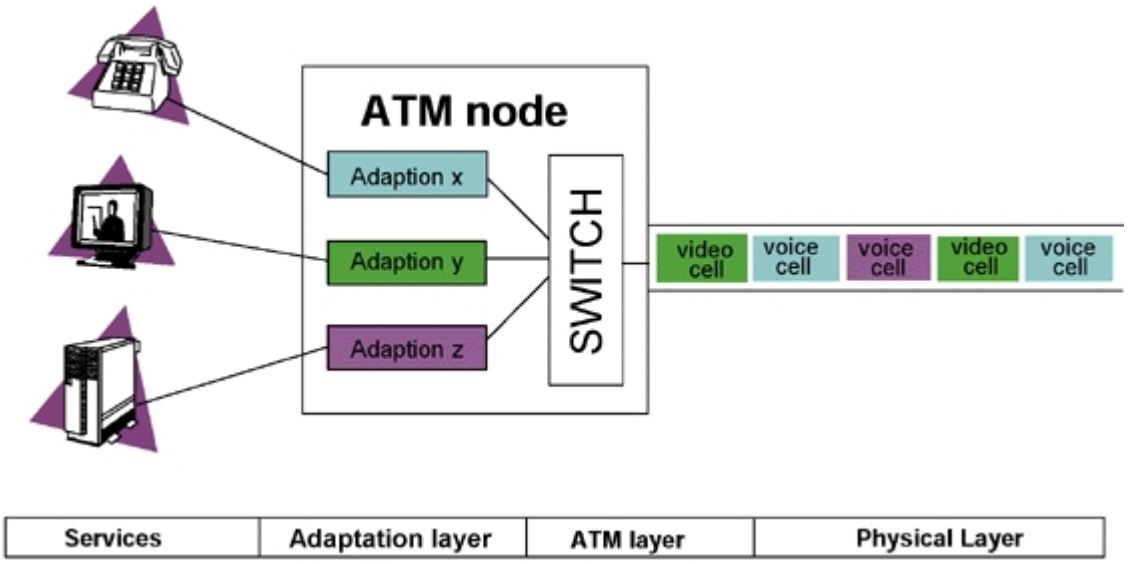
High speed network technology used for LAN, MAN and WAN

Like frame relay it is connection oriented technology which creates and uses fixed channel

Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM

Asynchronous Transfer Mode



Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standard-approved technology for speeding up network traffic flow and making things easier to manage.MPLS involves setting up a specific path for a given

Licensed to Berend Post berend.post@it-university.nl

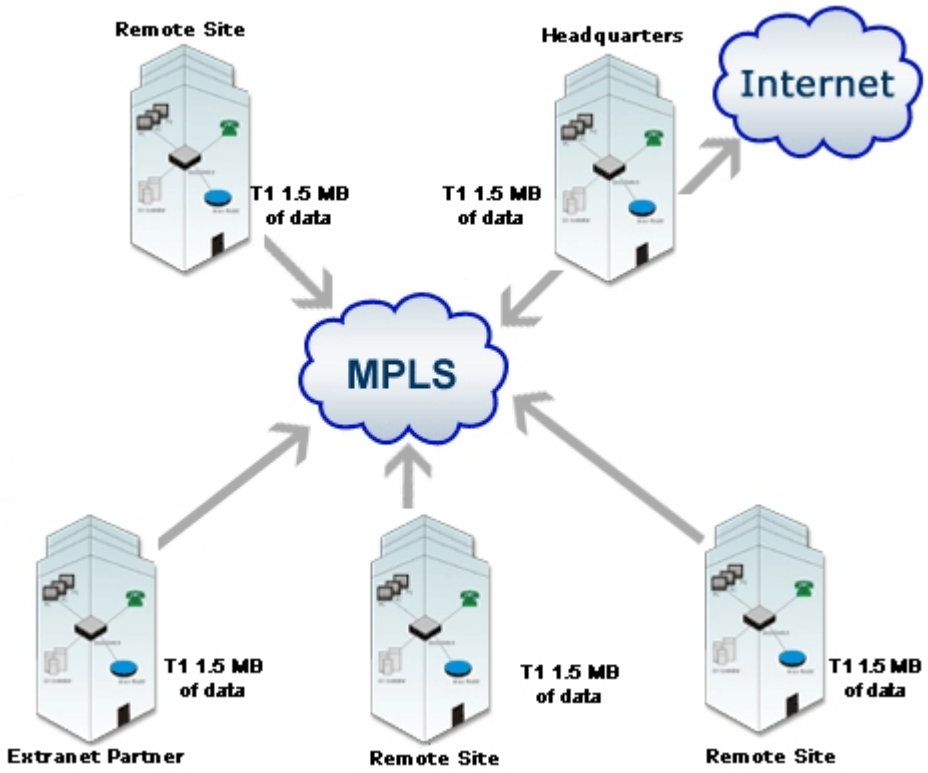
sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to.

MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols.

In reference to the Open Systems Interconnection, or OSI model, MPLS allows most packets to be forwarded at Layer 2 (switching) level rather than at the Layer 3 (routing) level.

In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS



The following answers are incorrect:

DCE - Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

DME – Not a valid frame relay technique

DLE – Not a valid frame relay technique

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

Question 2204

Which of the following is the BEST way to determine the effectiveness of a recently installed intrusion detection system (IDS)?

- ☐ Implement access control.
- ☒ Conduct attack simulation.
- ☐ Review audit logs.
- ☐ Inspect IDS configuration.

Question 2205

Which of the following line media would provide the BEST security for a telecommunication network?

- ☐ broadband network digital transmission
- ☐ Baseband network
- ☐ Dial-up
- ☒ Dedicated lines

Explanation:

Explanation:

Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

Question 2206

Which of the following is the MOST beneficial outcome of testing an incident response plan?

- ☐ The plan is enhanced to reflect the findings of the test.
- ☐ Test plan results are documented.
- ☒ Incident response time is improved.
- ☐ The response includes escalation to senior management.

Licensed to Berend Post berend.post@it-university.nl

Question 2207

Which of the following methods would BEST help detect unauthorized disclosure of confidential documents sent over corporate email?

- ☐ Installing firewalls on the corporate network
- ☐ Requiring all users to encrypt documents before sending
- ☒ Monitoring all emails based on pre-defined criteria
- ☐ Reporting all outgoing emails that are marked as confidential

Question 2208

An IS auditor has observed gaps in the data available to the organization for detecting incidents. Which of the following would be the BEST recommendation to improve the organization's security incident response capability?

- ☐ Document procedures for incident escalation.
- ☐ Document procedures for incident classification.
- ☐ Correlate security logs collected from multiple sources.
- ☒ Centralize alerts and security log information.

Question 2209

What is the most effective means of determining that controls are functioning properly within an operating system?

- ☐ Interview with computer operator
- ☒ Review of software control features and/or parameters
- ☐ Review of operating system manual
- ☐ Interview with product vendor

Explanation:

Various operating system software products provide parameters and options for the tailoring of the system and activation of features such as activity logging. Parameters are important in determining how a system runs because they allow a standard piece of software to be customized to diverse environments. The reviewing of software control features and/or parameters is the most effective means of determining how controls are functioning within an operating system and of assessing and operating system's integrity.

The operating system manual should provide information as to what settings can be used but will not likely give any hint as to how parameters are actually set. The product vendor and computer operator are not necessarily aware of the detailed setting of all parameters.

The review of software control features and/or parameters would be part of your security audit. A security audit is typically performed by an independent third party to the management of the system. The audit determines the degree with which the required controls are implemented.

Licensed to Berend Post berend.post@it-university.nl

A security review is conducted by the system maintenance or security personnel to discover vulnerabilities within the system. A vulnerability occurs when policies are not followed, miscon figurations are present, or flaws exist in the hardware or software of the system. System reviews are sometimes referred to as a vulnerability assessment.

Reference(s) used for this question:

Schneider, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Security Operations, Page 1054, for users with the Kindle edition look at Locations 851-855

and

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 102).

Question 2210

Which of the following IS audit recommendations would BEST help to ensure appropriate mitigation will occur on control weaknesses identified during an audit?

- ☒ Assign actions to responsible personnel and follow up.
- ☐ Report on progress to the audit committee.
- ☐ Perform a cost-benefit analysis on remediation strategy.
- ☐ Implement software to input the action points from the IS audit.

Question 2211

Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's information security awareness program?

- ☒ Security awareness training is not included as part of the onboarding process for new hires.
- ☐ The number of security incidents logged by employees to the help desk has increased in the past year.
- ☐ Training quizzes are designed and run by a third-party company under a contract with the organization.
- ☐ Security awareness training is run via the organization's enterprise-wide e-learning portal.

Licensed to Berend Post berend.post@it-university.nl

Question 2212

Which of the following refers to any authentication protocol that requires two independent ways to establish identity and privileges?

- ☐ Strong-factor authentication
- ☒ Two-factor authentication
- ☐ Dual-password authentication
- ☐ Two-passphrases authentication
- ☐ Dual-keys authentication
- ☐ Rich-factor authentication

Explanation:

Explanation:

Two-factor authentication (T-FA) refers to any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as the other factor. In fact, using more than one factor is also called strong authentication. On the other hand, using just one factor is considered by some weak authentication.

Question 2213

For an organization which uses a VoIP telephony system exclusively, the GREATEST concern associated with leaving a connected telephone in an unmonitored public area is the possibility of:

- ☐ connectivity issues when used with an analog local exchange carrier
- ☒ unauthorized use leading to theft of services and financial loss
- ☐ network compromise due to the introduction of malware
- ☐ theft or destruction of an expensive piece of electronic equipment

Question 2214

An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

- ☐ Allow changes to be made only with the DBA user account.
- ☐ Make changes to the database after granting access to a normal user account.
- ☒ Use the DBA user account to make changes, log the changes and review the change log the following day.
- ☐ Use the normal user account to make changes, log the changes and review the change log the following day.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The use of a database administrator (DBA) user account is normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

Question 2215

Capacity management enables organizations to:

- ☐ establish the capacity of network communication links.
- ☐ determine business transaction volumes.
- ☐ forecast technology trends.
- ☒ identify the extent to which components need to be upgraded.

Question 2216

Facilitating telecommunications continuity by providing redundant combinations of local carrier T- 1 lines, microwaves and/or coaxial cables to access the local communication loop:

- ☒ last-mile circuit protection.
- ☐ long-haul network diversity.
- ☐ diverse routing.
- ☐ alternative routing.

Explanation:

Explanation:

The method of providing telecommunication continuity through the use of many recovery facilities, providing redundant combinations of local carrier T-Is, microwave and/or coaxial cable to access the local communication loop in the event of a disaster, is called last-mile circuit protection.

Providing diverse long-distance network availability utilizing T-I circuits among major long- distance carriers is called long-haul network diversity. This ensures long-distance access should any one carrier experience a network failure. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

Licensed to Berend Post berend.post@it-university.nl

Question 2217

Which of the following is the key benefit of control self-assessment (CSA)?

- ☒ Management ownership of the internal controls supporting business objectives is reinforced.
- ☐ Audit expenses are reduced when the assessment results are an input to external audit work.
- ☐ Improved fraud detection since internal business staff are engaged in testing controls
- ☐ Internal auditors can shift to a consultative approach by using the results of the assessment.

Explanation:

Explanation:

The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance.

Reducing audit expenses is not a key benefit of control self-assessment (CSA). improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

Question 2218

Which of the following is a telecommunication device that translates data from digital to analog form and back to digital?

- ☐ Multiplexer
- ☒ Modem
- ☐ Protocol converter
- ☐ Concentrator

Explanation:

A modem is a device that translates data from digital form and then back to digital for communication over analog lines.

Source: Information Systems Audit and Control Association,

Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

Licensed to Berend Post berend.post@it-university.nl

Question 2219

What are often the primary safeguards for systems software and data?

- ☐ Administrative access controls
- ☒ Logical access controls
- ☐ Physical access controls
- ☐ Detective access controls

Explanation:

Explanation:

Logical access controls are often the primary safeguards for systems software and datA.

Question 2220

Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

- ☐ all threats can be completely removed.
- ☒ a cost-effective, built-in resilience can be implemented.
- ☐ the recovery time objective can be optimized.
- ☐ the cost of recovery can be minimized.

Explanation:

Explanation:

It is critical to initially identify information assets that can be made more resilient to disasters, e.g., diverse routing, alternate paths or multiple communication carriers. It is impossible to remove all existing and future threats. The optimization of the recovery time objective and efforts to minimize the cost of recovery come later in the development of the disaster recovery strategy.

Question 2221

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- ☒ Review and, where necessary, upgrade firewall capabilities
- ☐ Install modems to allow remote maintenance support access
- ☐ Create a physically distinct network to handle VoIP traffic
- ☐ Redirect all VoIP traffic to allow clear text logging of authentication credentials

Explanation:

Explanation:

Firewalls used as entry points to a Voice-over Internet Protocol (VoIP) network should be VoIP-capable. VoIP network services such as H.323 introduce complexities that are likely to strain the capabilities of older firewalls. Allowing for remote support access is an important consideration. However, a virtual private network (VPN) would offer a more secure means of enabling this access

Licensed to Berend Post berend.post@it-university.nl

than reliance on modems. Logically separating the VoIP and data network is a good idea. Options such as virtual LANS (VLA.NS), traffic shaping, firewalls and network address translation (NAT) combined with private IP addressing can be used; however, physically separating the networks will increase both cost and administrative complexity. Transmitting or storing clear text information, particularly sensitive information such as authentication credentials, will increase network vulnerability. When designing a VoIP network, it is important to avoid introducing any processing that will unnecessarily increase latency since this will adversely impact VoIP quality.

Question 2222

The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

- ☐ that there will be too many alerts for system administrators to verify.
- ☐ decreased network performance due to IPS traffic.
- ☒ the blocking of critical systems or services due to false triggers.
- ☐ reliance on specialized expertise within the IT organization.

Explanation:

Explanation:

An intrusion prevention system (IPS) prevents a connection or service based on how it is programmed to react to specific incidents. If the packets are coming from a spoofed address and the IPS is triggered based on previously defined behavior, it may block the service or connection of a critical internal system. The other choices are risks that are not as severe as blocking critical systems or services due to false triggers.

Question 2223

In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

- ☐ CASE tools
- ☐ Embedded data collection tools
- ☐ Heuristic scanning tools
- ☒ Trend/variance detection tools

Explanation:

Explanation:

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

Licensed to Berend Post berend.post@it-university.nl

Question 2224

Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

- ☒ Assess the impact of patches prior to installation.
- ☐ Ask the vendors for a new software version with all fixes included.
- ☐ install the security patch immediately.
- ☐ Decline to deal with these vendors in the future.

Explanation:

Explanation:

The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions withal fixes included are not always available and a full installation could be time consuming. Declining to deal with vendors does not take care of the flaw.

Question 2225

Following request for proposal (RFP) responses, a project seeking to acquire a new application system has identified a short list of vendors. At this point, the IS auditor should:

- ☐ encourage contact with current users of the vendor's products
- ☐ perform a detailed cost-benefit exercise on the proposed application
- ☒ require that contract terms include a right-to-audit clause
- ☐ recommend performing system integration tests

Question 2226

Which of the following is NOT a disadvantage of Single Sign On (SSO)?

- ☐ Support for all major operating system environment is difficult
- ☐ The cost associated with SSO development can be significant
- ☐ SSO could be single point of failure and total compromise of an organization asset
- ☒ SSO improves an administrator's ability to manage user's account and authorization to all associated system

Explanation:

Single sign-on (SSO)is a Session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

SSO Advantages include

Multiple passwords are no longer required

Licensed to Berend Post berend.post@it-university.nl

It improves an administrator's ability to manage user's accounts and authorization to all associated systems

It reduces administrative overhead in resetting forgotten password over multiple platforms and applications

It reduces time taken by users to logon into multiple application and platform

SSO Disadvantages include

Support for all major operating system is difficult

The cost associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary

The centralize nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information asset.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 332

Question 2227

Which of the following is a guiding best practice for implementing logical access controls?

- ☐ Implementing the Biba Integrity Model
- ☒ Access is granted on a least-privilege basis, per the organization's data owners
- ☐ Implementing the Take-Grant access control model
- ☐ Classifying data according to the subject's requirements

Explanation:

Explanation:

Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

Licensed to Berend Post berend.post@it-university.nl

Question 2228

The BEST method of proving the accuracy of a system tax calculation is by:

- ☐ detailed visual review and analysis of the source code of the calculation programs
- ☐ recreating program logic using generalized audit software to calculate monthly totals.
- ☒ preparing simulated transactions for processing and comparing the results to predetermined results.
- ☐ automatic flowcharting and analysis of the source code of the calculation programs.

Explanation:

Explanation:

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

Question 2229

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

- ☒ The risks associated with the use of the products are periodically assessed
- ☐ The latest version of software is listed for each product
- ☐ Due to licensing issues the list does not contain open source software
- ☐ After hours' support is offered

Explanation:

Explanation:

Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C and D are possible considerations but would not be the most important.

Question 2230

During a security audit, which of the following is MOST important to review to ensure data confidentiality is managed?

- ☒ Access controls
- ☐ Data flows
- ☐ Access log monitoring
- ☐ Network configuration

Licensed to Berend Post berend.post@it-university.nl

Question 2231

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- ☐ Test data run
- ☐ Code review
- ☒ Automated code comparison
- ☐ Review of code migration procedures

Explanation:

Explanation:

An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

Question 2232

A top-down approach to the development of operational policies will help ensure:

- ☒ that they are consistent across the organization.
- ☐ that they are implemented as a part of risk assessment.
- ☐ compliance with all policies.
- ☐ that they are reviewed periodically.

Explanation:

Explanation:

Deriving lower level policies from corporate policies {a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

Question 2233

The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will MOST likely:

- ☒ increase.
- ☐ decrease.
- ☐ remain the same.
- ☐ be unpredictable.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Due to the additional cost of disaster recovery planning (DRP) measures, the cost of normal operations for any organization will always increase after a DRP implementation, i.e., the cost of normal operations during a nondisaster period will be more than the cost of operations during a nondisaster period when no disaster recovery plan was in place.

Question 2234

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

- ☐ inheritance
- ☐ Dynamic warehousing
- ☒ Encapsulation
- ☐ Polymorphism

Explanation:

Explanation:

Encapsulation is a property of objects, and it prevents accessing either properties or methods that have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.

Question 2235

Reports to the executive level concerning IT performance should focus on:

- ☐ third-party compliance with organizational practices.
- ☐ IT performance in relation to operational improvements.
- ☒ IT deliverables against organizational strategies.
- ☐ capacity planning effectiveness within the organization.

Question 2236

Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

- ☐ Minimum operating requirements
- ☒ Acceptable data loss
- ☐ Mean time between failures
- ☐ Acceptable time for recovery

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Recovery time objectives (RTOs) are the acceptable time delay in availability of business operations, while recovery point objectives (RPOs) are the level of data loss/reworking an organization is willing to accept. Mean time between failures and minimum operating requirements help in defining recovery strategies.

Question 2237

You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you're seeing a series of bits placed in the "Urgent Pointer" field of a TCP packet. This is only 16 bits which isn't much but it concerns you because:

- ☒ This could be a sign of covert channeling in bank network communications and should be investigated.
- ☐ It could be a sign of a damaged network cable causing the issue.
- ☐ It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
- ☐ It is normal traffic because sometimes the previous fields 16-bit checksum value can over run into the urgent pointer's 16-bit field causing the condition.

Explanation:

Explanation:

The Urgent Pointer is used when some information has to reach the server ASAP. When the TCP/IP stack at the other end sees a packet using the Urgent Pointer set, it is duty bound to stop all ongoing activities and immediately send this packet up the stack for immediate processing. Since the packet is plucked out of the processing queue and acted upon immediately, it is known as an Out Of Band (OOB)packet and the data is called Out Of Band (OOB) data.

The Urgent Pointer is usually used in Telnet, where an immediate response (e.g. the echoing of characters) is desirable.

Covert Channels are not directly synonymous with backdoors. A covert channel is simply using a communication protocol in a way it was not intended to be used or sending data without going through the proper access control mechanisms or channels. For example, in a Mandatory Access Control systems a user at secret has found a way to communicate information to a user at Confidential without going through the normal channels.

In this case the Urgent bit could be used for a few reasons:

1. It could be to attempt a Denial of service where the host receiving a packet with the Urgent bit set will give immediate attention to the request and will be in wait state until the urgent message is receive, if the sender does not send the urgent message then it will simply sit there doing nothing until it times out. Some of the TCP/IP stacks used to have a 600 seconds time out, which means that

Licensed to Berend Post berend.post@it-university.nl

for 10 minutes nobody could use the port. By sending thousands of packet with the URGENT flag set, it would create a very effective denial of service attack.

2. It could be used as a client server application to transmit data back and forward without going through the proper channels. It would be slow but it is possible to use reserved fields and bits to transmit data outside the normal communication channels.

The other answers are incorrect

The following reference(s) were/was used to create this question:

http://www.fas.org/irp/nsa/rainbow/tg030.htm document covering the subject of covert channels

and also see:

http://gray-world.net/papers.shtml which is a large collection of documents on Covert Channels

Question 2238

What is the PRIMARY benefit to executive management when audit, risk, and security functions are aligned?

- ☐ More efficient incident handling
- ☐ Reduced number of assurance reports
- ☒ More effective decision making
- ☐ More timely risk reporting

Question 2239

To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

- ☐ online terminals are placed in restricted areas.
- ☐ online terminals are equipped with key locks.
- ☐ ID cards are required to gain access to online terminals.
- ☒ online access is terminated after a specified number of unsuccessful attempts.

Explanation:

Explanation:

The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through the guessing of IDs and passwords. The

Licensed to Berend Post berend.post@it-university.nl

other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

Question 2240

Which of the following security control is intended to avoid an incident from occurring?

- ☐ Deterrent
- ☒ Preventive
- ☐ Corrective
- ☐ Recovery

Explanation:

Explanation:

Preventive controls are intended to avoid an incident from occurring

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For

 Licensed to Berend Post berend.post@it-university.nl

example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that

 Licensed to Berend Post berend.post@it-university.nl

authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

 Licensed to Berend Post berend.post@it-university.nl

Deterrent - Deterrent controls are intended to discourage a potential attacker

Corrective - Corrective control fixes components or systems after an incident has occurred

Recovery - Recovery controls are intended to bring the environment back to regular operations

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 2241

Within a security governance framework, which of the following is the MOST important characteristic of the information security committee? The committee:

- ☐ conducts frequent reviews of the security policy.
- ☒ includes a mix of members from all levels of management.
- ☐ has a clearly defined charter and meeting protocols.
- ☐ has established relationships with external professionals.

Question 2242

Which of the following would normally be the MOST reliable evidence for an auditor?

- ☒ A confirmation letter received from a third party verifying an account balance
- ☐ Assurance from line management that an application is working as designed
- ☐ Trend data obtained from World Wide Web (Internet) sources
- ☐ Ratio analysts developed by the IS auditor from reports supplied by line management

Explanation:

Explanation:

Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

Licensed to Berend Post berend.post@it-university.nl

Question 2243

Which of the following is a directive control?

- ☐ Establishing an information security operations team
- ☐ Updating data loss prevention software
- ☒ Implementing an information security policy
- ☐ Configuring data encryption software

Question 2244

There are many known weaknesses within an Intrusion Detection System (IDS). Which of the following is NOT a limitation of an IDS?

- ☐ Weakness in the identification and authentication scheme.
- ☐ Application level vulnerability.
- ☐ Backdoor into application
- ☒ Detect zero day attack.

Explanation:

Detecting zero day attack is an advantage of IDS system making use of behavior or heuristic detection.

It is important to read carefully the question. The word "NOT" was the key word.

Intrusion Detection System are somewhat limited in scope, they do not address the following:

Weakness in the policy definition

Application-level vulnerability

Backdoor within application

Weakness in identification and authentication schemes

Also, you should know the information below for your CISA exam:

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies.

Broad category of IDS includes:

1. Network Based IDS

Licensed to Berend Post berend.post@it-university.nl

2. Host Based IDS

Network Based IDS

They identify attack within the monitored network and issue a warning to the operator.

If a network based IDS is placed between the Internet and the firewall, it will detect all the attack attempts whether or not they enter the firewall

Network Based IDS are blinded when dealing with encrypted traffic

Host Based IDS

They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack.

They can detect the modification of executable programs, detect the detection of files and issue a warning when an attempt is made to use a privilege account.

They can monitor traffic after it is decrypted and they supplement the Network Based IDS.

Types of IDS includes:

Statistical Based IDS – This system needs a comprehensive definition of the known and expected behavior of system

Neural Network – An IDS with this feature monitors the general patterns of activity and traffic on the network, and create a database. This is similar to statistical model but with added self-learning functionality.

Signature Based IDS – These IDS system protect against detected intrusion patterns. The intrusive pattern they can identify are stored in the form of signature.

The following were incorrect answers:

The other options mentioned are all limitations of an IDS.

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 Page number 346 and 347

Question 2245

Which of the following will MOST effectively help to manage the challenges associated with end user-developed application systems?

- ☐ Developing classifications based on risk
- ☐ Introducing redundant support capacity
- ☐ Prohibiting creation of executable files
- ☒ Applying control practices used by IT

Question 2246

Which of the following can degrade network performance?

- ☐ Superfluous use of redundant load-sharing gateways
- ☐ Increasing traffic collisions due to host congestion by creating new collision domains
- ☐ Inefficient and superfluous use of network devices such as switches
- ☒ Inefficient and superfluous use of network devices such as hubs

Explanation:

Explanation:

Inefficient and superfluous use of network devices such as hubs can degrade network performance.

Question 2247

An organization has recently incorporated robotic process automation. Which of the following would be of GREATEST concern to an IS auditor?

- ☐ Controls have not been tested
- ☐ A governance structure has not been implemented
- ☒ A risk assessment has not been conducted
- ☐ The adoption rate for the new technology has been low

Licensed to Berend Post berend.post@it-university.nl

Question 2248

Which of the following is the MOST effective control for emergency changes to application programs?

- ☒ Processing the change through change control with review of the change the following day
- ☐ Keeping a sealed envelope containing a password that operators can use to make emergency changes
- ☐ Periodically checking the application program libraries to detect whether unauthorized changes have been made
- ☐ Preparing and approving program change forms before the changes are made

Question 2249

During a review of system access, an IS auditor notes that an employee who has recently changed roles within the organization still has previous access rights. The auditor's NEXT step should be to:

- ☒ determine the reason why access rights have not been revoked.
- ☐ recommend a control to automatically update access rights.
- ☐ direct management to revoke current access rights.
- ☐ determine if access rights are in violation of software licenses.

Question 2250

Which of the following would BEST support a business case to implement a data leakage prevention (DLP) solution?

- ☐ An unusual upward trend in outbound email volume
- ☐ Lack of visibility into previous data leakage incidents
- ☐ Industry benchmark of DLP investments
- ☒ A risk assessment on the threat of data leakage

Question 2251

Which of the following practices associated with capacity planning provides the GREATEST assurance that future incidents related to server performance will be prevented?

- ☐ Anticipating current service level agreements (SLAs) will remain unchanged
- ☒ Prorating the current processing workloads
- ☐ Negotiating agreements to acquire required cloud services
- ☐ Duplicating existing disk drive systems to improve redundancy and data storage

Licensed to Berend Post berend.post@it-university.nl

Question 2252

Screening router inspects traffic through examining:

- ☒ message header.
- ☐ virus payload
- ☐ message content
- ☐ attachment type
- ☐ None of the choices.

Explanation:

Explanation:

The simplest and almost cheapest type of firewall is a packet filter that stops messages with inappropriate network addresses. It usually consists of a screening router and a set of rules that accept or reject a message based on information in the message header.

Question 2253

The extent to which data will be collected during an IS audit should be determined based on the:

- ☐ availability of critical and required information.
- ☐ auditor's familiarity with the circumstances.
- ☐ auditee's ability to find relevant evidence.
- ☒ purpose and scope of the audit being done.

Explanation:

Explanation:

The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and the scope of the audit should not be limited by the auditee's ability to find relevant evidence.

Question 2254

Over the long term, which of the following has the greatest potential to improve the security incident response process?

- ☐ A walkthrough review of incident response procedures
- ☒ Postevent reviews by the incident response team
- ☐ Ongoing security training for users
- ☐ Documenting responses to an incident

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Postevent reviews to find the gaps and shortcomings in the actual incident response processes will help to improve the process over time. Choices A, C and D are desirable actions, but postevent reviews are the most reliable mechanism for improving security incident response processes.

Question 2255

An organization has shifted from a bottom-up approach to a top-down approach in the development of IT policies. This should result in:

- ☐ a synthesis of existing operational policies
- ☐ greater consistency across the organization
- ☐ greater adherence to best practices
- ☒ a more comprehensive risk assessment plan

Question 2256

Buffer overflow aims primarily at corrupting:

- ☐ system processor
- ☐ network firewall
- ☒ system memory
- ☐ disk storage
- ☐ None of the choices.

Explanation:

Explanation:

A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

Question 2257

Which of the following is the BEST indication that an information security program is effective?

- ☒ The number of reported and confirmed security incidents has increased after awareness training.
- ☐ The security awareness program was developed following industry best practices.
- ☐ The security team has performed a risk assessment to understand the organization's risk appetite.
- ☐ The security team is knowledgeable and uses the best available tools.

Licensed to Berend Post berend.post@it-university.nl

Question 2258

Which of the following factor is LEAST important in the measurement of critical success factors of productivity in the SDLC phases?

- ☐ Dollar Spent per use
- ☐ Number of transactions per month
- ☐ Number of transactions per user
- ☒ Number of occurrences of fraud/misuse detection

Explanation:

The LEAST is the keyword used in this question, You need to find out a LEAST important factor in the measurement of the productivity.

For the CISA exam you should know the table below which contains information about measurement of a critical success factor.

Measurement of Critical Success Factors

Productivity

Dollars spent per use

Number of transactions per month

Number of transactions per user

Quality

Number of discrepancies

Number of disputes

Number of occurrences of fraud/misuse detection

Economic value

Total processing time reduction

Momentary value of administration costs

Customer service

Turnaround time for customer question handling

Frequency of useful communication to user.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

The other options presented are more important in the measurement of critical success factor of the productivity.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 159

Question 2259

Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

- ☒ Built-in alternative routing
- ☐ Completing full system backup daily
- ☐ A repair contract with a service provider
- ☐ A duplicate machine alongside each server

Explanation:

Explanation: Alternative routing would ensure the network would continue if a server is lost or if a link is severed as message rerouting could be automatic. System backup will not afford immediate protection. The repair contract is not as effective as perm a nentalte (native routing). Standby servers will not provide continuity if a link is severed.

Question 2260

Which of the following management decisions presents the GREATEST risk associated with data leakage?

- ☒ Security awareness training is not provided to staff.
- ☐ There is no requirement for desktops to be encrypted.
- ☐ Security policies have not been updated in the past year.
- ☐ Staff are allowed to work remotely.

Question 2261

Which of the following protocol does NOT work at Network interface layer in TCP/IP model?

- ☐ ICMP
- ☒ DNS
- ☐ ARP
- ☐ Internet protocol

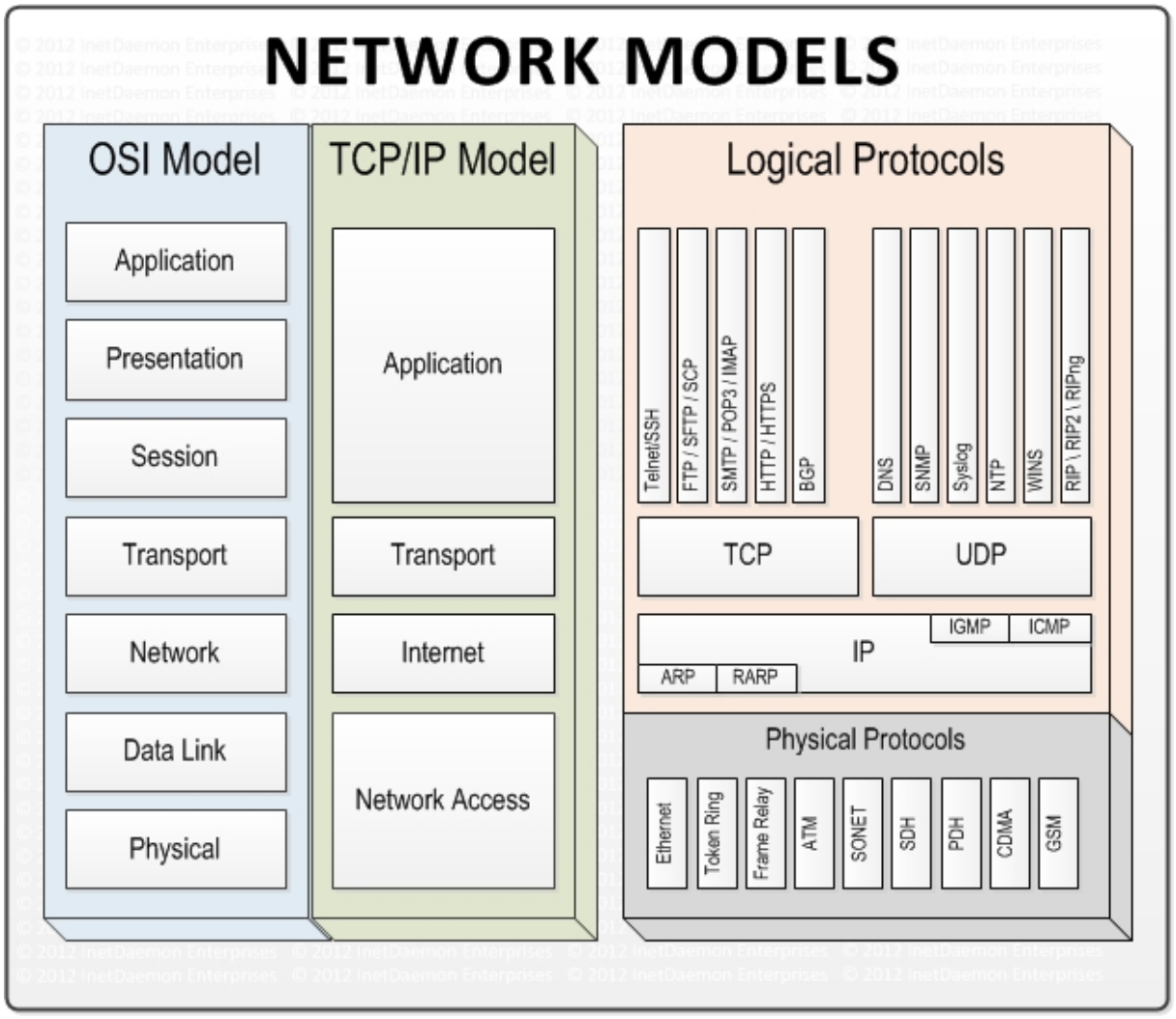
Explanation:

Licensed to Berend Post berend.post@it-university.nl

The NOT is the keyword used in the question. You need to find out a protocol which does not work at network interface layer in TCP/IP model. DNS protocol works at application layer of a TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Licensed to Berend Post berend.post@it-university.nl

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

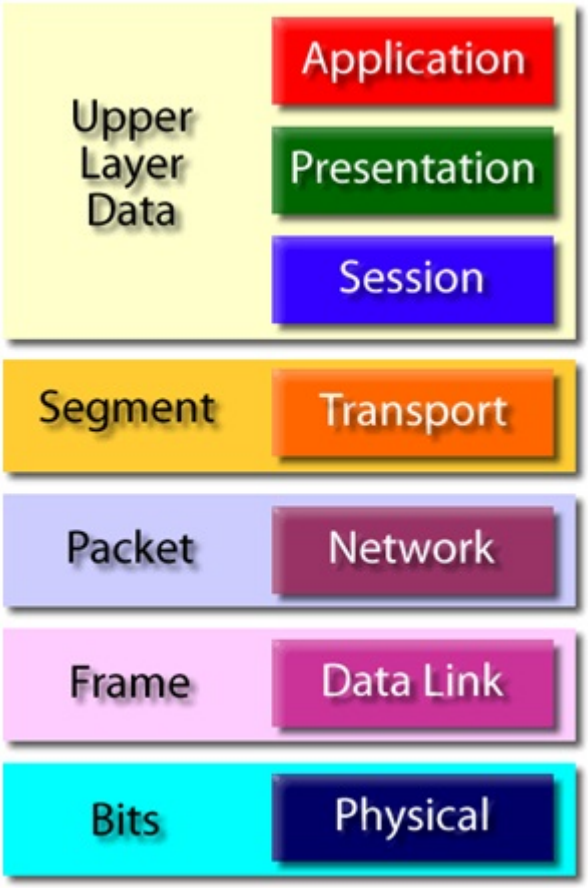
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

Licensed to Berend Post berend.post@it-university.nl

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :



Protocol Data Unit - PDU

The following answers are incorrect:

ICMP, ARP and Internet protocol works at Network interface layer of a TCP/IP model.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 272

Licensed to Berend Post berend.post@it-university.nl

Question 2262

What are the different types of Audits?

- ☒ Compliance, financial, operational, forensic and integrated
- ☐ Compliance, financial, operational, G9 and integrated
- ☐ Compliance, financial, SA1, forensic and integrated
- ☐ Compliance, financial, operational, forensic and capability

Explanation:

Compliance, financial, operational, forensic and integrated are different types of audit.

For your exam you should know the information below:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization's accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit

Licensed to Berend Post berend.post@it-university.nl

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data

Licensed to Berend Post berend.post@it-university.nl

integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance, financial, operational, forensic and integrated are different types of audits. G9, SA1 and capability are not the audit types.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 47

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

Licensed to Berend Post berend.post@it-university.nl

http://www.investorwords.com/16445/forensic_audit.html

Question 2263

An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

- ☐ Recommend that an additional comprehensive BCP be developed.
- ☒ Determine whether the BCPs are consistent.
- ☐ Accept the BCPs as written.
- ☐ Recommend the creation of a single BCP.

Explanation:

Explanation:

Depending on the complexity of the organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan; however, each plan should be consistent with other plans to have a viable business continuity planning strategy.

Question 2264

During a business process re-engineering (BPR) program, IT can assist with:

- ☐ total cost of ownership.
- ☒ focusing on value-added tasks.
- ☐ segregation of duties.
- ☐ streamlining of tasks.

Question 2265

When storing data archives off-site, what must be done with the data to ensure data completeness?

- ☐ The data must be normalized.
- ☐ The data must be validated.
- ☐ The data must be parallel-tested.
- ☒ The data must be synchronized.

Explanation:

Explanation:

When storing data archives off-site, data must be synchronized to ensure data completeness

Licensed to Berend Post berend.post@it-university.nl

Question 2266

Which of the following is MOST important to consider when assessing the scope of privacy concerns for an IT project?

- ☒ Applicable laws and regulations
- ☐ End user access rights
- ☐ Business requirements
- ☐ Classification of data

Question 2267

Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

- ☒ Encrypt the hard disk with the owner's public key.
- ☐ Enable the boot password (hardware-based password).
- ☐ Use a biometric authentication device.
- ☐ Use two-factor authentication to logon to the notebook.

Explanation:

Explanation:

Only encryption of the data with a secure key will prevent the loss of confidential information. In such a case, confidential information can be accessed only with knowledge of the owner's private key, which should never be shared. Choices B, C and D deal with authentication and not with confidentiality of information. An individual can remove the hard drive from the secured laptop and install it on an unsecured computer, gaining access to the data.

Question 2268

An organization’s current end-user computing practices include the use of a spreadsheet for financial statements. Which of the following is the GREATEST concern?

- ☒ Formulas are not protected against unintended changes.
- ☐ The spreadsheet contains numerous macros.
- ☐ Operational procedures have not been reviewed in the current fiscal year.
- ☐ The spreadsheet is not maintained by IT.

Licensed to Berend Post berend.post@it-university.nl

Question 2269

An IS auditor observes that the CEO has full access to the enterprise resource planning (ERP) system. The IS auditor should FIRST:

- ☐ accept the level of access provided as appropriate
- ☐ recommend that the privilege be removed
- ☐ ignore the observation as not being material to the review
- ☒ document the finding as a potential risk

Question 2270

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- ☐ Integrating of assurance efforts
- ☐ Automation of controls
- ☒ Standardization of compliance requirements
- ☐ Documentation of control procedures

Question 2271

Which of the following is the MOST effective mechanism for ensuring that critical IT operational problems are reported to executive management in a timely manner?

- ☐ Regular meetings
- ☐ Escalation procedures
- ☒ Service level monitoring
- ☐ Periodic status reports

Question 2272

Which of the following observations would an IS auditor consider the GREATEST risk when conducting an audit of a virtual server farm for potential software vulnerabilities?

- ☐ The hypervisor is updated quarterly.
- ☐ Guest operating systems are updated monthly.
- ☒ Antivirus software has been implemented on the guest operating system only.
- ☐ A variety of guest operating systems operate on one virtual server.

Licensed to Berend Post berend.post@it-university.nl

Question 2273

For a company that outsources payroll processing, which of the following is the BEST way to ensure that only authorized employees are paid?

- ☒ The company's bank reconciliations should be independently prepared and checked.
- ☐ Employees should receive pay statements showing gross pay, net pay, and deductions.
- ☐ Only payroll employees should be given the password for data entry and report retrieval.
- ☐ Electronic payroll reports should be independently reviewed.

Question 2274

In a complex IS environment, which of the following tasks should be performed by the data owner?

- ☐ Perform technical database maintenance.
- ☐ Perform data restoration when necessary.
- ☒ Review data classifications periodically.
- ☐ Test the validity of backup data.

Question 2275

A database audit reveals an issue with the way data ownership for client data is defined. Which of the following roles should be accountable for this finding?

- ☐ Business management
- ☒ Database administrator
- ☐ Information security management
- ☐ Privacy manager

Question 2276

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

- ☒ Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
- ☐ The contingency plan for the organization cannot effectively test controlled access practices.
- ☐ Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
- ☐ Removing access for those who are no longer authorized is complex.

Explanation:

Explanation:

The concept of piggybacking compromises all physical control established. Choice B would be of minimal concern in a disaster recovery environment. Items in choice C are not easily duplicated.

Licensed to Berend Post berend.post@it-university.nl

Regarding choice D, while technology is constantly changing, card keys have existed for some time and appear to be a viable option for the foreseeable future.

Question 2277

A Trojan horse's payload would almost always take damaging effect immediately.

- ☐ True
- ☒ False

Explanation:

Explanation:

Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to immediate yet undesirable effects, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals.

Question 2278

Which of the following would BEST enable effective IT resource management?

- ☐ Assessing the risk associated with IT resources
- ☐ Outsourcing IT processes and activities
- ☒ Establishing business priorities
- ☐ Automating business processes

Question 2279

Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

- ☒ implement column- and row-level permissions
- ☐ Enhance user authentication via strong passwords
- ☐ Organize the data warehouse into subject matter-specific databases
- ☐ Log user access to the data warehouse

Explanation:

Explanation:Choice A specifically addresses the question of sensitive data by controlling what information users can access. Column-level security prevents users from seeing one or more attributes on a table. With row-level security a certain grouping of information on a table is restricted; e.g., if a table held details of employee salaries, then a restriction could be put in place to ensure that, unless specifically authorized, users could not view the salaries of executive staff. Column- and row-level security can be achieved in a relational database by allowing users to access logical representations of data rather than physical tables. This 'fine-grained' security model is likely to offer the best balance between information protection while still supporting a wide range of analytical and reporting uses. Enhancing user authentication via strong passwords is a security

Licensed to Berend Post berend.post@it-university.nl

control that should apply to all users of the data warehouse and does not specifically address protection of sensitive data. Organizing a data warehouse into subject-specific databases is a potentially useful practice but, in itself, does not adequately protect sensitive data. Database-level security is normally too 'coarse' a level to efficiently and effectively protect information. For example, one database may hold information that needs to be restricted such as employee salary and customer profitability details while other information such as employee department may need to be legitimately a accessed by a large number of users. Organizing the data warehouse into subject matter-specific databases is similar to user access in that this control should generally apply. Extra attention could be devoted to reviewing access to tables with sensitive data, but this control is not sufficient without strong preventive controls at the column and row level. For choice D, logging user access is important, but it is only a detective control that will not provide adequate protection to sensitive information.

Question 2280

Who is ultimately responsible and accountable for reviewing user access to systems?

- ☐ Systems security administrators
- ☐ Data custodians
- ☒ Data owners
- ☐ Information systems auditors

Explanation:

Explanation:

Data owners are ultimately responsible and accountable for reviewing user access to systems.

Question 2281

Which of the following is the MOST likely cause of a successful firewall penetration?

- ☐ Use of a Trojan to bypass the firewall
- ☐ Loophole in firewall vendor's code
- ☐ Virus infection
- ☒ Firewall misconfiguration by the administrator

Question 2282

Which of the following is the MOST effective control when granting temporary access to vendors?

- ☐ Vendor access corresponds to the service level agreement (SLA).
- ☒ User accounts are created with expiration dates and are based on services provided.
- ☐ Administrator access is provided for a limited period.
- ☐ User IDs are deleted when the work is completed.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The most effective control is to ensure that the granting of temporary access is based on services to be provided and that there is an expiration date (hopefully automated) associated with each ID. The SLA may have a provision for providing access, but this is not a control; it would merely define the need for access. Vendors require access for a limited period during the time of service. However, it is important to ensure that the access during this period is monitored. Deleting these user, I Dafter the work is completed is necessary, but if not automated, the deletion could be overlooked.

Question 2283

As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains a significant change or addition of new functionality?

- ☒ Major software Release
- ☐ Minor software Release
- ☐ Emergency software release
- ☐ General software Release

Explanation:

A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner.

Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Software Release management is a process through which software is made available to user. Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.

 Licensed to Berend Post berend.post@it-university.nl

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release – Not a valid type of software release.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 244

Question 2284

When developing metrics to measure the contribution of IT to the achievement of business goals, the MOST important consideration is that the metrics:

- ☐ measure the effectiveness of IT controls in the achievement of IT strategy.
- ☒ provide quantitative measurement of IT initiatives in relation with business targets.
- ☐ are expressed in terms of how IT risk impacts the achievement of business goals.
- ☐ are used by similar industries to measure the effect of IT on business strategy.

Licensed to Berend Post berend.post@it-university.nl

Question 2285

An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's FIRST course of action?

- ☒ Validate that there has been an incident
- ☐ Notify the business process owner
- ☐ Shut down the server in an organized manner
- ☐ Inform senior management of the incident

Question 2286

During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

- ☒ the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
- ☐ there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
- ☐ the database will immediately stop execution and lose more information.
- ☐ the database will no longer accept input data.

Explanation:

Explanation:

When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction data. This will normally cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be unacceptable. Choice B is incorrect, since a system can recover the corrupted external key by reindexing the table. Choices C and D would not result from a corrupted foreign key.

Question 2287

The role of the certificate authority (CA) as a third party is to:

- ☐ provide secured communication and networking services based on certificates.
- ☐ host a repository of certificates with the corresponding public and secret keys issued by that CA.
- ☐ act as a trusted intermediary between two communication partners.
- ☒ confirm the identity of the entity owning a certificate issued by that CA.

Explanation:

Explanation:

The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would

Licensed to Berend Post berend.post@it-university.nl

not be archived at the CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.

Question 2288

An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

- ☒ References from other customers
- ☐ Service level agreement (SLA) template
- ☐ Maintenance agreement
- ☐ Conversion plan

Explanation:

Explanation:

An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows-issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

Question 2289

To test the integrity of the data in the accounts receivable master file, an IS auditor is particularly interested in reviewing customers with balances over $400,000. The selection technique the IS auditor would use to obtain such a sample is called:

- ☐ random selection.
- ☒ systematic selection.
- ☐ discovery selection.
- ☐ stratification.

Question 2290

An IS auditor has been asked to audit a complex system with computerized and manual elements. Which of the following should be identified FIRST?

- ☐ Manual controls
- ☐ System risks
- ☐ Programmed controls
- ☒ Input validation

Licensed to Berend Post berend.post@it-university.nl

Question 2291

Which of the following is the PRIMARY advantage of the IT portfolio management approach over the balanced scorecard approach when managing IT investments?

- ☐ The influence of qualitative factors on investment decisions.
- ☐ Agility in adjusting investment decisions.
- ☐ Incorporation of organizational strategy in investment decisions.
- ☒ Use of the organization's risk appetite in investment decisions.

Question 2292

An IS auditor has just completed a physical access review of the organization's primary data center. Which of the following weaknesses should be of MOST concern?

- ☐ Metal keys are used for access.
- ☐ Backups of video cameras are corrupt.
- ☒ There is no mantrap at the main door.
- ☐ There is no manual logging for visitors.

Question 2293

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- ☐ Proper authentication
- ☒ Proper identification AND authentication
- ☐ Proper identification
- ☐ Proper identification, authentication, AND authorization

Explanation:

Explanation:

If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

Question 2294

Input/output controls should be implemented for which applications in an integrated systems environment?

- ☐ The receiving application
- ☐ The sending application
- ☒ Both the sending and receiving applications
- ☐ Output on the sending application and input on the receiving application

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

Question 2295

Which of the following communication modes should be of GREATEST concern to an IS auditor evaluating end-user networking?

- ☐ System-to-system
- ☒ Peer-to-peer
- ☐ Host-to-host
- ☐ Client-to-server

Question 2296

An organization is currently replacing its accounting system. Which of the following strategies will BEST minimize risk associated with the loss of data integrity from the upgrade?

- ☐ Pilot implementation
- ☒ Functional integration testing
- ☐ Fallback contingency
- ☐ Parallel implementation

Question 2297

Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

- ☐ Processing power
- ☐ Volume of data
- ☒ Key distribution
- ☐ Complexity of the algorithm

Explanation:

Explanation:

Symmetric key encryption requires that the keys be distributed. The larger the user group, the more challenging the key distribution. Symmetric key cryptosystems are generally less complicated and, therefore, use less processing power than asymmetric techniques, thus making it ideal for encrypting a large volume of data. The major disadvantage is the need to get the keys into the hands of those with whom you want to exchange data, particularly in e-commerce environments, where customers are unknown, untrusted entities

Licensed to Berend Post berend.post@it-university.nl

Question 2298

Which of the following BEST contributes to the successful management of security incidents?

- ☐ Tested controls
- ☒ Established procedures
- ☐ Established policies
- ☐ Current technologies

Question 2299

An operations manager has recently moved to internal audit. Which of the following would be of GREATEST concern when assigning audit projects to this individual?

- ☐ A control within the audit scope was implemented by the operations manager six months ago.
- ☐ A control within the audit scope was downgraded to low risk by the operations manager six months ago.
- ☐ The owner of a process within the audit scope worked for the operations manager six month ago.
- ☒ A system within the audit scope is supported by an emerging technology for which the operations manager lacks experience.

Question 2300

Which of the following satisfies a two-factor user authentication?

- ☐ Iris scanning plus fingerprint scanning
- ☐ Terminal ID plus global positioning system (GPS)
- ☒ A smart card requiring the user's PIN
- ☐ User ID along with password

Explanation:

Explanation:

A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). Proving who the user is usually requires a biometrics method, such as fingerprint, iris scan or voice verification, to prove biology. This is not a two-factor user authentication, because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. The use of an ID and password (what the user knows) is a single- factor user authentication.

Licensed to Berend Post berend.post@it-university.nl

Question 2301

Which of the following are the PRIMARY considerations when determining the timing of remediation testing?

- ☐ The level of management and business commitment to implementing agreed action plans
- ☐ The difficulty of scheduling resources and availability of management for a follow-up engagement
- ☐ The availability and competencies of control owners for implementing the agreed action
- ☒ The significance of the reported findings and the impact if corrective actions are not taken

Question 2302

An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

- ☐ Use a process-based maturity model such as the capability maturity model (CMM)
- ☐ Regular monitoring of task-level progress against schedule
- ☐ Extensive use of software development tools to maximize team productivity
- ☒ Postiteration reviews that identify lessons learned for future use in the project

Explanation:

Explanation:

A key tenet of the Agile approach to software project management is team learning and the use of team learning to refine project management and software development processes as the project progresses. One of the best ways to achieve this is that, at the end of each iteration, the team considers and documents what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics.

Additionally, less importance is placed on formal paper- based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of greater importance.

Licensed to Berend Post berend.post@it-university.nl

Question 2303

An organization transmits large amounts of data from one internal system to another. The IS auditor is reviewing the quality of the data at the originating point. Which of the following should the auditor verify FIRST?

- ☒ The data has been encrypted.
- ☐ The data transformation is accurate.
- ☐ The data extraction process is completed.
- ☐ The source data is accurate.

Question 2304

Which of the following is a PRIMARY responsibility of an information security governance committee?

- ☐ Approving the purchase of information security technologies
- ☐ Approving the information security awareness training strategy
- ☒ Reviewing the information security strategy
- ☐ Analyzing information security policy compliance reviews

Question 2305

Which of the following is MOST important for an IS auditor to verify during a disaster recovery audit?

- ☒ Disaster recovery tests are carries out.
- ☐ Regular backups are made and stored offsite.
- ☐ The disaster recovery plan is updated on a regular basis.
- ☐ Media are stored in fireproof cabinets.

Question 2306

Information for detecting unauthorized input from a terminal would be BEST provided by the:

- ☐ console log printout.
- ☒ transaction journal.
- ☐ automated suspense file listing.
- ☐ user error report.

Explanation:

Explanation:

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, while the user error report would only list input that resulted in an edit error.

Licensed to Berend Post berend.post@it-university.nl

Question 2307

Which of the following is the BEST way to address potential data privacy concerns associated with inadvertent disclosure of machine identifier information contained within security logs?

- ☐ Only collect logs from servers classified as business critical.
- ☒ Limit the use of logs to only those purposes for which they were collected.
- ☐ Limit log collection to only periods of increased security activity.
- ☐ Restrict the transfer of log files from host machine to online storage.

Question 2308

Which of the following findings should be of GREATEST concern for an IS auditor when auditing the effectiveness of a phishing simulation test administered for staff members?

- ☐ Staff members were not notified about the test beforehand.
- ☐ Test results were not communicated to staff members.
- ☒ Staff members who failed the test did not receive follow-up education.
- ☐ Security awareness training was not provided prior to the test.

Question 2309

During a review of an insurance company's claims system, the IS auditor learns that claims for specific medical procedures are acceptable only from females. This is an example of a:

- ☐ key verification.
- ☐ completeness check.
- ☐ reasonableness check.
- ☒ logical relationship check.

Question 2310

An IS audit team is evaluating the documentation related to the most recent application user-access review performed by IT and business management. It is determined the user list was not system-generated. Which of the following should be the GREATEST concern?

- ☒ Source of the user list reviewed
- ☐ Availability of the user list reviewed
- ☐ Confidentiality of the user list reviewed
- ☐ Completeness of the user list reviewed

Licensed to Berend Post berend.post@it-university.nl

Question 2311

An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

- ☐ Permanent table-space allocation
- ☐ Commitment and rollback controls
- ☒ User spool and database limit controls
- ☐ Read/write access log controls

Explanation:

Explanation:

User spool limits restrict the space available for running user queries. This prevents poorly formed queries from consuming excessive system resources and impacting general query performance. Limiting the space available to users in their own databases prevents them from building excessively large tables. This helps to control space utilization which itself acts to help performance by maintaining a buffer between the actual data volume stored and the physical device capacity. Additionally, it prevents users from consuming excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run overnight and are optimized for performance purposes), in a data warehouse, since you are not running online transactions, commitment and rollback does not have an impact on performance. The other choices are not as likely to be the root cause of this performance issue.

Question 2312

An external audit team is deciding whether to rely on internal audit's work for an annual compliance audit. Which of the following is the GREATEST consideration when making this decision?

- ☐ Independence of the internal audit department from management's influence
- ☐ Professional certifications held by the internal audit team members
- ☐ Years of experience each of the internal auditors have in performing compliance audits
- ☒ The level of documentation maintained by internal audit and the methods used to collect evidence

Question 2313

A PRIMARY benefit derived by an organization employing control self-assessment (CSA) techniques is that CSA:

- ☒ can identify high-risk areas for detailed review.
- ☐ allows IS auditors to independently assess risk.
- ☐ can be used as a replacement for traditional audits.
- ☐ allows management to relinquish responsibility for control.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Choice B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Choice C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

Question 2314

During an audit of a data center, an IS auditor's BEST way to gain an understanding of physical security controls is to:

- ☐ review the data center's physical security procedures.
- ☐ contact the alarm vendor and identify where alarms are installed in the data center.
- ☒ take a tour of the facility and identify physical security controls.
- ☐ obtain the engineering plans for the building and identify points of entry.

Question 2315

Which of the following statement correctly describes the difference between black box testing and white box testing?

- ☒ Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
- ☐ White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
- ☐ White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
- ☐ White box and black box testing focuses on the effectiveness of the software program logic

Explanation:

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Licensed to Berend Post berend.post@it-university.nl

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user’s desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:

The other options presented does not provides correct difference between black box and white box testing.

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 Page number 167

Question 2316

A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

- ☒ use of the user's electronic signature by another person if the password is compromised.
- ☐ forgery by using another user's private key to sign a message with an electronic signature.
- ☐ impersonation of a user by substitution of the user's public key with another person's public key.
- ☐ forgery by substitution of another person's private key on the computer.

Explanation:

Explanation:

The user's digital signature is only protected by a password. Compromise of the password would enable access to the signature. This is the most significant risk. Choice B would require subversion of the public key infrastructure mechanism, which is very difficult and least likely.

Choice C would require that the message appear to have come from a different person and therefore the true user's credentials would not be forged. Choice D has the same consequence as choice C.

Question 2317

An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

- ☐ increase the frequency for data replication between the different department systems to ensure timely updates.
- ☐ Centralize all request processing in one department to avoid parallel processing of the same request.
- ☒ Change the application architecture so that common data is held in just one shared database for all departments.
- ☐ implement reconciliation controls to detect duplicates before orders are processed in the systems.

Explanation:

Explanation:

Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannot be eliminated completely because parallel data entry is still possible. Business requirements will most likely dictate where data processing activities are performed. Changing the business structure to solve an IT problem is not practical or politically

Licensed to Berend Post berend.post@it-university.nl

feasible. Detective controls do not solve the problem of duplicate processing, and would require that an additional process be implemented to handle the discovered duplicates.

Question 2318

Which of the following testing method examines internal structure or working of an application?

- ☒ White-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Explanation:

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT).

White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system–level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements.

For your exam you should know the information below:

Alpha and Beta Testing - An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

Licensed to Berend Post berend.post@it-university.nl

White box testing - Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing - An integrity based form of testing associated with testing components of an information system's “functional” operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing -The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user’s desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following answers are incorrect:

Parallel Testing - This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Regression Testing -The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Licensed to Berend Post berend.post@it-university.nl

Pilot Testing -A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 167

Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

Question 2319

Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

- ☐ Change management
- ☐ Backup and recovery
- ☐ incident management
- ☒ Configuration management

Explanation:

Explanation:

The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new release fail, the baseline will provide a point to which to return. The other choices do not provide the processes necessary for establishing software release baselines and are not related to software release baselines.

Question 2320

Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?

- ☐ Defining the business recovery plan with the IT service provider
- ☐ Requiring an external security audits of the IT service provider
- ☐ Defining information security requirements with internal IT
- ☒ Requiring regular reporting from the IT service provider

Licensed to Berend Post berend.post@it-university.nl

Question 2321

In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

- ☐ Maintaining system software parameters
- ☒ Ensuring periodic dumps of transaction logs
- ☐ Ensuring grandfather-father-son file backups
- ☐ Maintaining important data at an offsite location

Explanation:

Explanation:

Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

Question 2322

Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

- ☐ ensure the employee maintains a good quality of life, which will lead to greater productivity.
- ☒ reduce the opportunity for an employee to commit an improper or illegal act.
- ☐ provide proper cross-training for another employee.
- ☐ eliminate the potential disruption caused when an employee takes vacation one day at a time.

Explanation:

Explanation:

Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time, it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

Question 2323

Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

- ☒ SSL
- ☐ FTP
- ☐ SSH
- ☐ S/MIME

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The Secure Socket Layer (SSL) Protocol is primarily used to provide confidentiality to the information sent across clients and servers.

For your exam you should know the information below:

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmitted over a public network such as the Internet.

SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers.

SSL is included as part of both the Microsoft and Netscape browsers and most Web server products.

Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. Later on SSL uses a Session Key along a Symmetric Cipher for the bulk of the data.

TLS and SSL are an integral part of most Web browsers (clients) and Web servers. If a Web site is on a server that supports SSL, SSL can be enabled and specific Web pages can be identified as requiring SSL access. Any Web server can be enabled by using Netscape's SSLRef program library which can be downloaded for noncommercial use or licensed for commercial use.

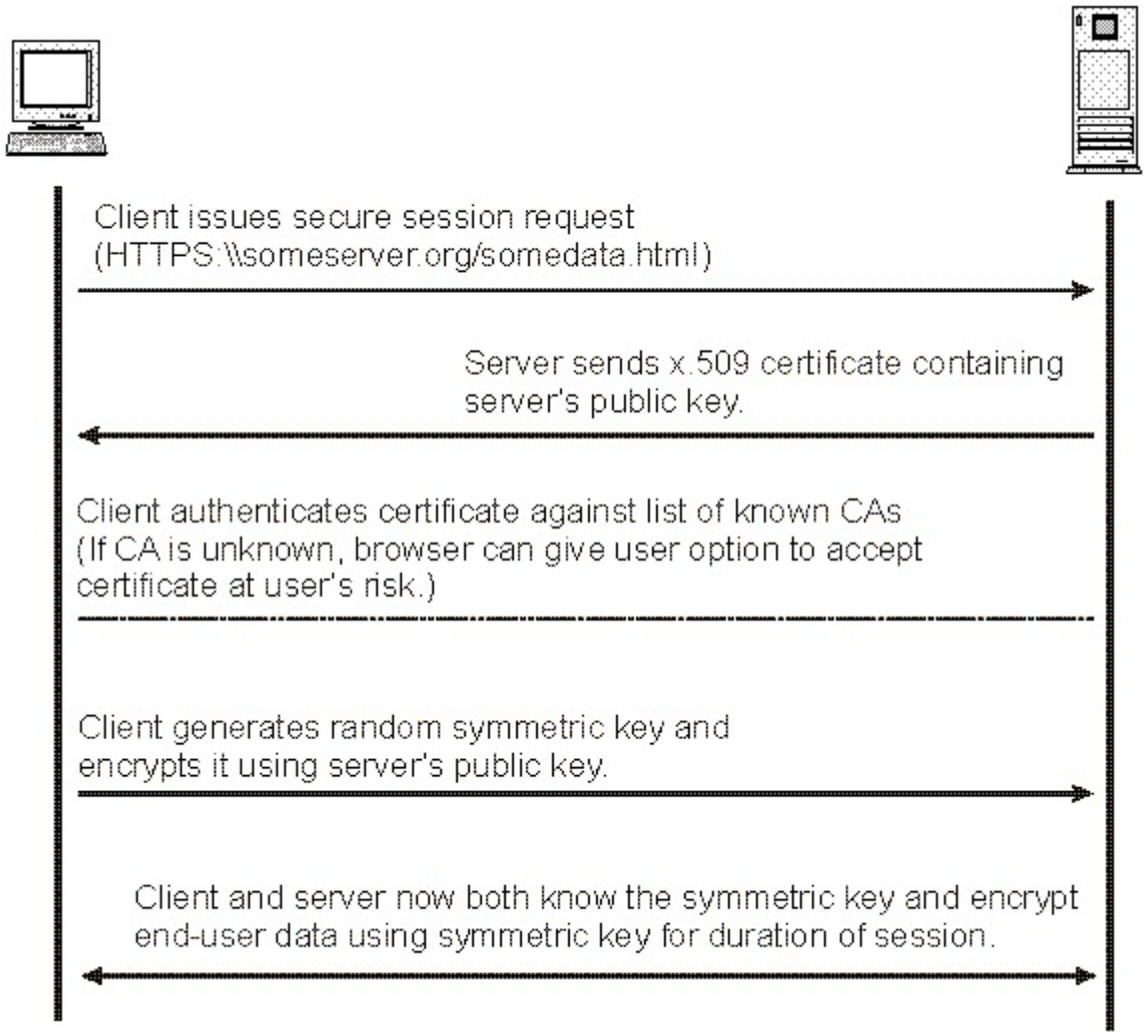
TLS and SSL are not interoperable. However, a message sent with TLS can be handled by a client that handles SSL but not TLS.

The SSL handshake

A HTTP-based SSL connection is always initiated by the client using a URL starting with https:// instead of with http://. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. A simplified overview of how the SSL handshake is processed is shown in the diagram below.

SSL Handshake

Licensed to Berend Post berend.post@it-university.nl



The client sends a client "hello" message that lists the cryptographic capabilities of the client (sorted in client preference order), such as the version of SSL, the cipher suites supported by the client, and the data compression methods supported by the client. The message also contains a 28-byte random number.

The server responds with a server "hello" message that contains the cryptographic method (cipher suite) and the data compression method selected by the server, the session ID, and another random number.

Note:

The client and the server must support at least one common cipher suite, or else the handshake fails. The server generally chooses the strongest common cipher suite.

The server sends its digital certificate. (In this example, the server uses X.509 V3 digital certificates with SSL.)

Licensed to Berend Post berend.post@it-university.nl

If the server uses SSL V3, and if the server application (for example, the Web server) requires a digital certificate for client authentication, the server sends a "digital certificate request" message. In the "digital certificate request" message, the server sends a list of the types of digital certificates supported and the distinguished names of acceptable certificate authorities.

The server sends a server "hello done" message and waits for a client response. Upon receipt of the server "hello done" message, the client (the Web browser) verifies the validity of the server's digital certificate and checks that the server's "hello" parameters are acceptable.

If the server requested a client digital certificate, the client sends a digital certificate, or if no suitable digital certificate is available, the client sends a "no digital certificate" alert. This alert is only a warning, but the server application can fail the session if client authentication is mandatory.

The client sends a "client key exchange" message. This message contains the pre-master secret, a 46-byte random number used in the generation of the symmetric encryption keys and the message authentication code (MAC) keys, encrypted with the public key of the server.

If the client sent a digital certificate to the server, the client sends a "digital certificate verify" message signed with the client's private key. By verifying the signature of this message, the server can explicitly verify the ownership of the client digital certificate.

Note:

An additional process to verify the server digital certificate is not necessary. If the server does not have the private key that belongs to the digital certificate, it cannot decrypt the pre-master secret and create the correct keys for the symmetric encryption algorithm, and the handshake fails.

The client uses a series of cryptographic operations to convert the pre-master secret into a master secret, from which all key material required for encryption and message authentication is derived. Then the client sends a "change cipher spec" message to make the server switch to the newly negotiated cipher suite. The next message sent by the client (the "finished" message) is the first message encrypted with this cipher method and keys.

The server responds with a "change cipher spec" and a "finished" message of its own.

The SSL handshake ends, and encrypted application data can be sent.

The following answers are incorrect:

 Licensed to Berend Post berend.post@it-university.nl

FTP - File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

SSH - Secure Shell (SSH) is a cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively.

S/MIME - S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the Rivets-Shamir-Adelman encryption system. S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape and has also been endorsed by other vendors that make messaging products. RSA has proposed S/MIME as a standard to the Internet Engineering Task Force (IETF).

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352

Official ISC2 guide to CISSP CBK 3rd Edition Page number 256

http://publib.boulder.ibm.com/tividd/td/ITAME/SC32-1363-00/en_US/HTML/ss7aumst18.htm

Question 2324

An organization is considering replacing physical backup tapes stored offsite with real-time on-line backup to a storage area network (SAN) located in the primary data center. Which of the following is the GREATEST risk?

- ☐ Archived data may not satisfy data retention requirements
- ☒ A single disaster could cause significant data loss
- ☐ Backups may require excessive storage space
- ☐ Implementation could cause significant cost increases

Licensed to Berend Post berend.post@it-university.nl

Question 2325

Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

- ☐ Cross-references between policies and procedures
- ☒ Inclusion of mission and objectives
- ☐ Compliance with relevant regulations
- ☐ Consultation with management

Question 2326

Which of the following is the GREATEST concern when an organization allows personal devices to connect to its network?

- ☒ It is difficult to enforce the security policy on personal devices
- ☐ Help desk employees will require additional training to support devices.
- ☐ IT infrastructure costs will increase.
- ☐ It is difficult to maintain employee privacy.

Question 2327

The output of the risk management process is an input for making:

- ☐ business plans.
- ☐ audit charters.
- ☒ security policy decisions.
- ☐ software design decisions.

Explanation:

Explanation:

The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

Question 2328

If a database is restored from information backed up before the last system image, which of the following is recommended?

- ☐ The system should be restarted after the last transaction.
- ☒ The system should be restarted before the last transaction.
- ☐ The system should be restarted at the first transaction.
- ☐ The system should be restarted on the last transaction.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

Question 2329

An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

- ☐ Log all table update transactions.
- ☐ implement before-and-after image reporting.
- ☐ Use tracing and tagging.
- ☒ implement integrity constraints in the database.

Explanation:

Explanation:

Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

Question 2330

Which of the following is the GREATEST threat to Voice-over Internet Protocol (VoIP) related to privacy release?

- ☐ Incorrect routing
- ☒ Eavesdropping
- ☐ Call recording
- ☐ Denial of service

Question 2331

During the evaluation of a firm's newly established whistleblower system, an auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

- ☐ New employees have not been informed of the whistleblower policy.
- ☒ The whistleblower's privacy is not protected.
- ☐ The whistleblower system does not track the time and date of submission.
- ☐ The whistleblower system is only available during business hours.

Licensed to Berend Post berend.post@it-university.nl

Question 2332

Which of the following is the PRIMARY purpose of red team testing?

- ☒ To determine the organization's preparedness for an attack
- ☐ To confirm the risk profile of the organization
- ☐ To assess the vulnerability of employees to social engineering
- ☐ To establish a baseline incident response program

Question 2333

Which of the following is the PRIMARY objective of the IS audit function?

- ☒ Perform reviews based on standards developed by professional organizations.
- ☐ Reports to management on the functioning of internal controls.
- ☐ Certify the accuracy of financial data.
- ☐ Facilitate extraction of computer-based data for substantive testing.

Question 2334

When planning an application audit, it is MOST important to evaluate risk factors by interviewing:

- ☒ process owners.
- ☐ application owners.
- ☐ IT management.
- ☐ application users.

Question 2335

An information security risk analysis BEST assists an organization in ensuring that:

- ☐ cost-effective decisions are made with regard to which assets need protection
- ☒ the organization implements appropriate security technologies
- ☐ the infrastructure has the appropriate level of access control
- ☐ an appropriate level of funding is applied to security processes

Question 2336

Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

- ☐ Parity check
- ☐ Echo check
- ☐ Block sum check
- ☒ Cyclic redundancy check

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The cyclic redundancy check (CRC) can check for a block of transmitted data. The workstations generate the CRC and transmit it with the data. The receiving workstation computes a CRC and compares it to the transmitted CRC. if both of them are equal. Then the block is assumed error free, in this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. Inhigher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

Question 2337

An IS auditor should know information about different network transmission media. Which of the following transmission media is used for short distance transmission?

- ☒ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Satellite Radio Link

Explanation:

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Licensed to Berend Post berend.post@it-university.nl

Coaxial Cable

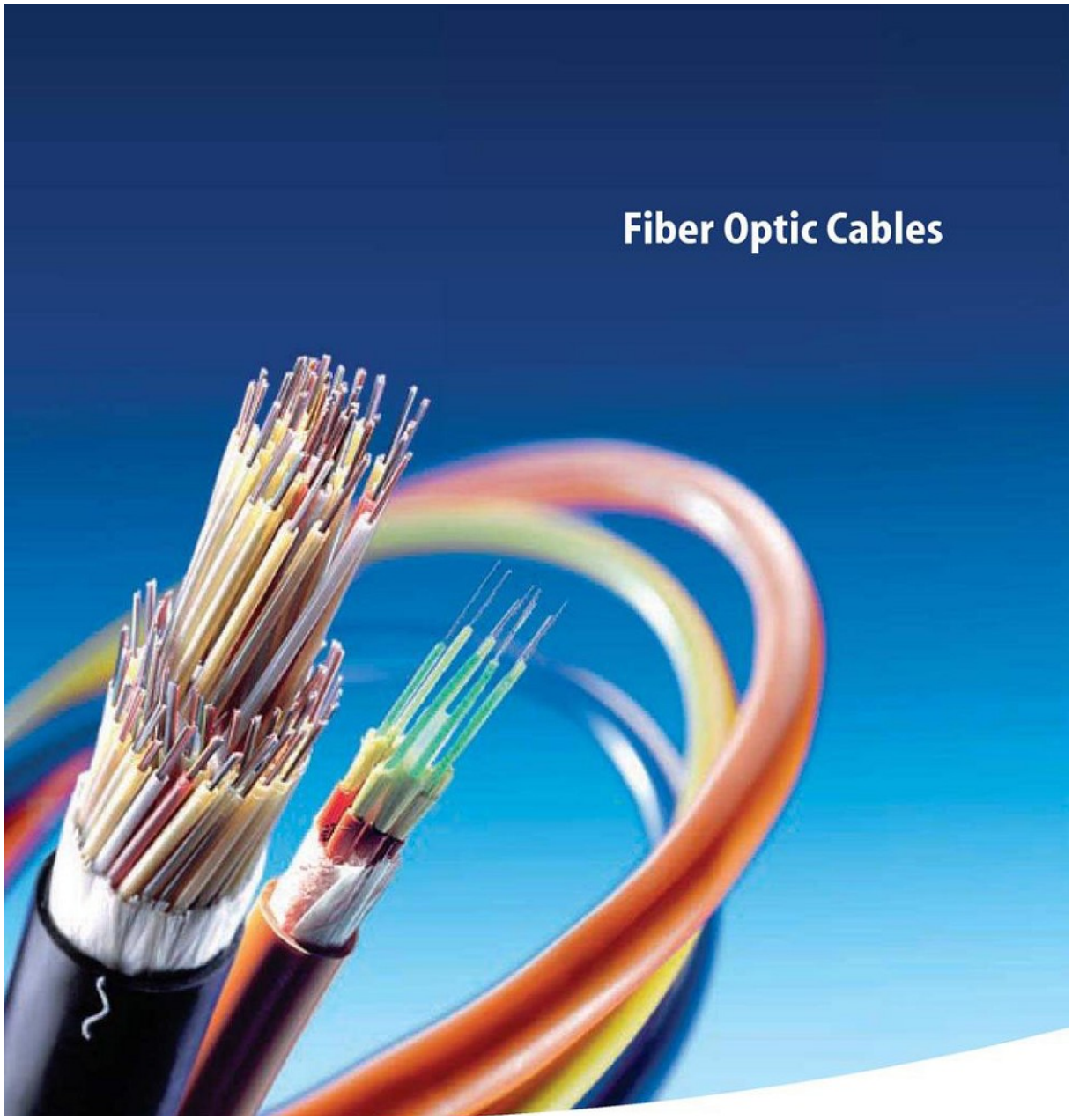
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Microwave radio system

Licensed to Berend Post berend.post@it-university.nl

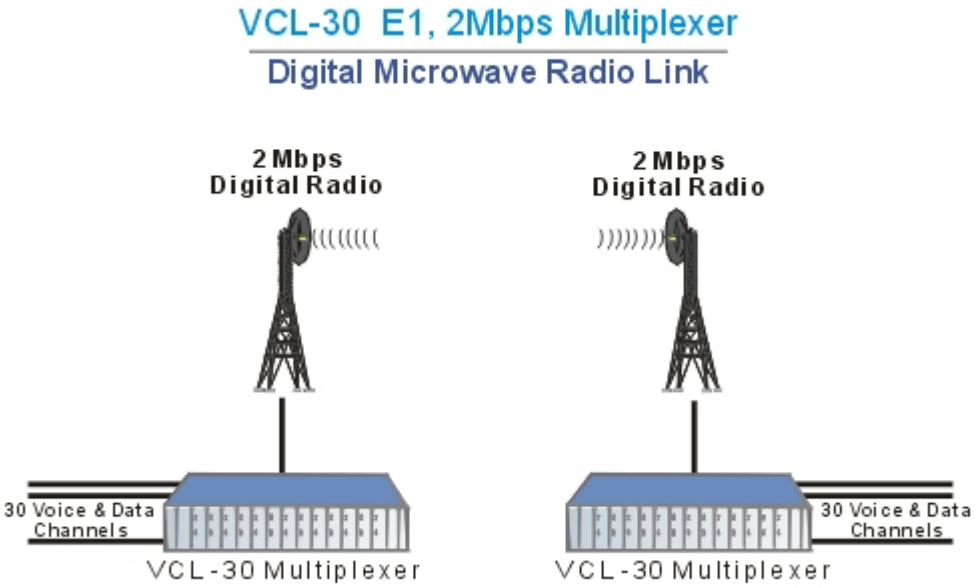
Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

Fiber optics - Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

Question 2338

An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?

- ☒ Review and evaluate the business continuity plan for adequacy
- ☐ Perform a full simulation of the business continuity plan
- ☐ Train and educate employees regarding the business continuity plan
- ☐ Notify critical contacts in the business continuity plan

Explanation:

Explanation:

The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization. There is no reason to notify the business continuity plan contacts at this time.

Question 2339

The MOST important reason for documenting all aspects of a digital forensic investigation is that documentation:

- ☐ provides traceability for independent investigation by third parties.
- ☒ ensures compliance with corporate incident response policies.
- ☐ ensures the process will be repeatable in future investigations.
- ☐ meets IT audit documentation standards.

Licensed to Berend Post berend.post@it-university.nl

Question 2340

What is the key distinction between encryption and hashing algorithms?

- ☐ Hashing algorithms ensure data confidentiality.
- ☒ Hashing algorithms are irreversible.
- ☐ Encryption algorithms ensure data integrity.
- ☐ Encryption algorithms are not irreversible.

Explanation:

Explanation:

A key distinction between encryption and hashing algorithms is that hashing algorithms are irreversible.

Question 2341

Which of the following access control situations represents the MOST serious control weakness?

- ☐ Computer operators have access to system level flowcharts.
- ☐ Programmers have access to development hardware.
- ☒ End users have access to program development tools.
- ☐ System developers have access to production data.

Question 2342

Which of the following is the MOST effective way to minimize the risk of a SQL injection attack?

- ☐ Reconfiguring content filtering settings
- ☐ Performing activity monitoring
- ☒ Using secure coding practices
- ☐ Implementing an intrusion detection tool

Question 2343

A business unit uses an e-commerce application with a strong password policy. Many customers complain that they cannot remember their passwords because they are too long and complex. The business unit states it is imperative to improve the customer experience. The information security manager should FIRST:

- ☐ change the password policy to improve the customer experience.
- ☐ recommend implementing two-factor authentication.
- ☒ research alternative secure methods of identity verification.
- ☐ evaluate the impact of the customer's experience on business revenue.

Licensed to Berend Post berend.post@it-university.nl

Question 2344

While planning a security audit, an IS auditor is made aware of a security review carried out by external consultants. It is MOST important for the auditor to:

- ☐ re-perform the security review.
- ☐ accept the findings and conclusions of the consultants.
- ☐ review similar reports issued by the consultants.
- ☒ assess the objectivity and competence of the consultants.

Question 2345

Which of the following types of transmission media provide the BEST security against unauthorized access?

- ☐ Copper wire
- ☐ Twisted pair
- ☒ Fiberoptic cables
- ☐ Coaxial cables

Explanation:

Explanation:

Fiberoptic cables have proven to be more secure than the other media. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

Question 2346

A company has purchased a rival organization and is looking to integrate security strategies. Which of the following is the GREATEST issue to consider?

- ☒ The organizations have different risk appetites
- ☐ Differing security technologies
- ☐ Differing security skills within the organizations
- ☐ Confidential information could be leaked

Question 2347

There are many types of audit logs analysis tools available in the market. Which of the following audit logs analysis tools will look for anomalies in user or system behavior?

- ☐ Attack Signature detection tool
- ☒ Variance detection tool
- ☐ Audit Reduction tool
- ☐ Heuristic detection tool

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Trend/Variance Detection tool are used to look for anomalies in user or system behavior. For example, if a user typically logs in at 9:00 am, but one day suddenly access the system at 4:30 am, this may indicate a security problem that may need to be investigated.

Other types of audit trail analysis tools should also be known for your CISA exam

The following were incorrect answers:

Audit Reduction tool - They are preprocessor designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tool can remove many audit records known to have little security significance.

Attack-signature detection tool - They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.

Heuristic detection tool - Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs with statistical analysis, which bases itself on the available data/statistics.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 336

and

http://en.wikipedia.org/wiki/Heuristic_analysis

Question 2348

Which of the following is the BEST evidence of the maturity of an organization's information security program?

- ☐ The number of reported incidents has increased.
- ☒ The information security department actively monitors security operations.
- ☐ The number of reported incidents has decreased.
- ☐ IT security staff implements strict technical security controls.

Licensed to Berend Post berend.post@it-university.nl

Question 2349

Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

- ☐ Function Point Analysis (FPA)
- ☐ GANTT
- ☐ Rapid Application Development (RAD)
- ☒ PERT

Explanation:

Explanation:

PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

Question 2350

Which of the following would BEST protect against web-based cross-domain attacks?

- ☐ Network addressing scheme
- ☐ Database hardening
- ☐ Encryption controls
- ☒ Application controls

Question 2351

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data- calculation procedures. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

Licensed to Berend Post berend.post@it-university.nl

Question 2352

When auditing third-party service providers, an IS auditor should be concerned with which of the following?

- ☐ Ownership of the programs and files
- ☐ A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster
- ☐ A statement of due care
- ☒ Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Explanation:

Explanation:

When auditing third-party service providers, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster.

Question 2353

To protect information assets, which of the following should be done FIRST?

- ☐ Restrict access to data
- ☐ Encrypt data
- ☒ Classify data
- ☐ Back up data

Question 2354

Relatively speaking, firewalls operated at the application level of the seven layer OSI model are:

- ☒ almost always less efficient.
- ☐ almost always less effective.
- ☐ almost always less secure.
- ☐ almost always less costly to setup.
- ☐ None of the choices.

Explanation:

Explanation:

Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU processing power.

Packet filters operate at the network layer and function more efficiently because they only look at the header part of a packet.

Licensed to Berend Post berend.post@it-university.nl

Question 2355

Which of the following would be the MOST efficient audit approach, given that a compliance-based approach was adopted in the previous year?

- ☐ Validate all applications using test data.
- ☐ Interview systems personnel to evaluate all automated controls.
- ☐ Evaluate the controls surrounding changes to programs.
- ☒ Perform a review of significant transactions posted within the system.

Question 2356

Which of the following function in traditional EDI translate data between the standard format and trading partner's propriety format?

- ☐ Communication handler
- ☐ Application Interface
- ☐ Application System
- ☒ EDI Translator

Explanation:

EDI Translator translates data between standard format (ANSI X12) and trading partner's propriety information.

For CISA Exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's computer system

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox services similar to post offices. The VAN receives all the outbound transactions from an organization, sort them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

EDI Interface -Interface function that manipulates and routes data between the application system and the communication handler. The interface consists of two components

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Licensed to Berend Post berend.post@it-university.nl

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping. Data mapping is the process by which data are extracted from EDI translation process and integrated with the data or process of receiving company.

3. Application System -The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN).

Application System -The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 178

Question 2357

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

- ☒ Deleting database activity logs
- ☐ Implementing database optimization tools
- ☐ Monitoring database usage
- ☐ Defining backup and recovery procedures

Explanation:

Explanation:

Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating

 Licensed to Berend Post berend.post@it-university.nl

control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

Question 2358

An IS auditor observes a system performance monitoring tool which states that a server critical to the organization averages high CPU utilization across a cluster of four virtual servers throughout the audit period. To determine if further investigation is required, an IS auditor should review:

- ☐ the system process activity log
- ☒ system baselines
- ☐ the number of CPUs allocated to each virtual machine
- ☐ organizational objectives

Question 2359

What should be done to determine the appropriate level of audit coverage for an organization's IT environment?

- ☐ determine the company's quarterly budget requirement.
- ☒ define an effective assessment methodology.
- ☐ calculate the company's yearly budget requirement.
- ☐ define an effective system upgrade methodology.
- ☐ define an effective network implementation methodology.

Explanation:

Explanation:

To determine the appropriate level of audit coverage for the organization's IT environment, you must define an effective assessment methodology and provide objective information to prioritize the allocation of audit resources properly.

Question 2360

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- ☒ Allocating resources
- ☐ Keeping current with technology advances
- ☐ Conducting control self-assessment
- ☐ Evaluating hardware needs

Explanation:

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating

Licensed to Berend Post berend.post@it-university.nl

hardware needs are not as critical as allocating resources during short-term planning for the IS department.

Question 2361

Which of the following is the BEST way to control the concurrent use of licensed software?

- ☐ User self-discipline.
- ☒ Monitor by system administrator.
- ☐ Surprise audit conducted by vendors.
- ☐ Metering software

Question 2362

Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?

1. Theft of service
2. Disclosure of information
3. Data Modifications
4. Denial of service
5. Traffic Analysis

- ☐ 3 and 4
- ☐ 4 and 5
- ☐ 1-4
- ☒ They are ALL risks associated with PBX

Explanation:

The NOT is a keyword used in the question. You need to find out the risks which are NOT associated with PBX. All the risk listed within the options are associated with PBX.

The threat of the PBX telephone system is many, depending on the goals of these attackers, and include:

Theft of service - Toll fraud, probably the most common of motives for attacker.

Disclosure of Information -Data disclosed without authorization, either by deliberate actionably accident. Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Licensed to Berend Post berend.post@it-university.nl

Data Modification -Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access – Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service -Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

Traffic Analysis – A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

All the risks presented in options are associated with PBX. So other options are not valid.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number356

Question 2363

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

- ☐ Concurrency controls
- ☐ Reasonableness checks
- ☒ Time stamps
- ☐ Referential integrity controls

Explanation:

Explanation:

Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

Licensed to Berend Post berend.post@it-university.nl

Question 2364

Malicious program code was found in an application and corrected prior to release into production. After the release, the same issue was reported. Which of the following is the IS auditor's BEST recommendation?

- ☐ Ensure the business signs off on end-to-end user acceptance test results.
- ☒ Ensure corrected program code is compiled in a dedicated server.
- ☐ Ensure change management reports are independently reviewed.
- ☐ Ensure programmers cannot access code after the completion of program edits.

Question 2365

Which of the following step of PDCA request a corrective actions on significant differences between the actual versus the planned result?

- ☐ Plan
- ☐ Do
- ☐ Check
- ☒ Act

Explanation:

Act - Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition."

The steps in each successive PDCA cycle are:

Licensed to Berend Post berend.post@it-university.nl

PLAN

Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

DO

Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

CHECK

Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

ACT

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

DO - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

CHECK - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 107

Question 2366

The purpose of a deadman door controlling access to a computer facility is primarily to:

- ☒ prevent piggybacking.
- ☐ prevent toxic gases from entering the data center.
- ☐ starve a fire of oxygen.
- ☐ prevent an excessively rapid entry to, or exit from, the facility.

Explanation:

Explanation:

The purpose of a deadman door controlling access to a computer facility is primarily intended to prevent piggybacking. Choices B and C could be accomplished with a single self-closing door. Choice D is invalid, as a rapid exit may be necessary in some circumstances, e.g., a fire.

Question 2367

A company has implemented an IT segregation of duties policy. In a role-based environment, which of the following roles may be assigned to an approach developer?

- ☐ IT operator
- ☐ Database administration
- ☐ System administration
- ☒ Emergency support

Licensed to Berend Post berend.post@it-university.nl

Question 2368

Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

- ☐ Certificate revocation list (CRL)
- ☒ Certification practice statement (CPS)
- ☐ Certificate policy (CP)
- ☐ PKI disclosure statement (PDS)

Explanation:

Explanation:

The CPS is the how-to part in policy-based PKI. The CRL is a list of certificates that have been revoked before their scheduled expiration date. The CP sets the requirements that are subsequently implemented by the CPS. The PDS covers critical items such as the warranties, limitations and obligations that legally bind each party.

Question 2369

To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

- ☒ the source routing field is enabled.
- ☐ it has a broadcast address in the destination field.
- ☐ a reset flag (RST) is turned on for the TCP connection.
- ☐ dynamic routing is used instead of static routing.

Explanation:

Explanation:

IP spoofing takes advantage of the source-routing option in the IP protocol. With this option enabled, an attacker can insert a spoofed source IP address. The packet will travel the network according to the information within the source-routing field, bypassing the logic in each router, including dynamic and static routing (choice D). Choices B and C do not have any relation to IP spoofing attacks. If a packet has a broadcast destination address (choice B), it will be sent to all addresses in the subnet. Turning on the reset flag (RST) (choice C) is part of the normal procedure to end a TCP connection.

Question 2370

To ensure authentication, confidentiality and integrity of a message, the sender should encrypt the hash of the message with the sender's:

- ☐ public key and then encrypt the message with the receiver's private key.
- ☒ private key and then encrypt the message with the receiver's public key.
- ☐ public key and then encrypt the message with the receiver's public key.
- ☐ private key and then encrypt the message with the receiver's private key.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

Question 2371

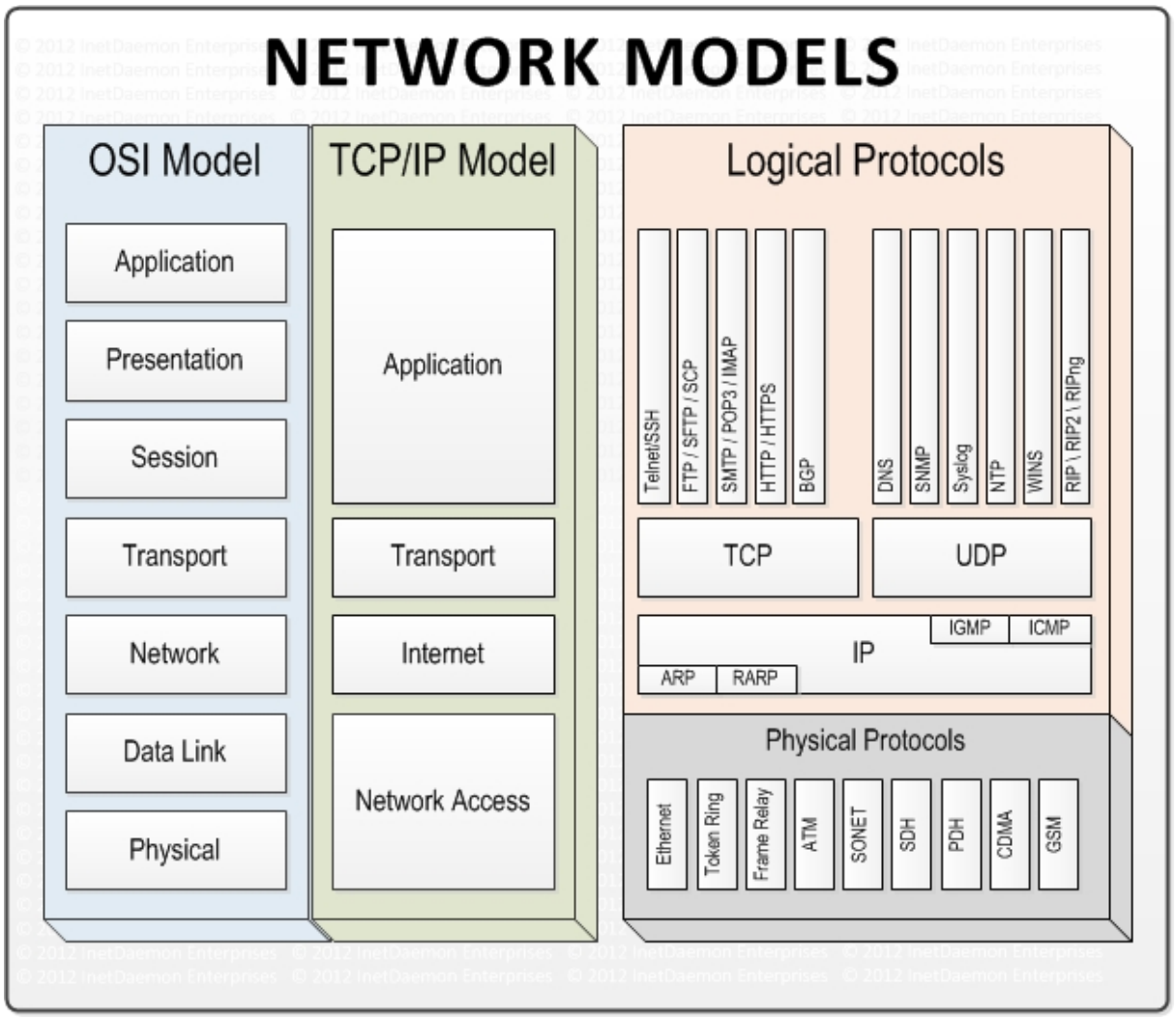
Which of the following is protocol data unit (PDU) of network interface layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☒ Packet
- ☐ Frame

Explanation:

For your exam you should know below information about TCP/IP model:

Network models



Layer 4. Application Layer

Licensed to Berend Post berend.post@it-university.nl

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or

Licensed to Berend Post berend.post@it-university.nl

optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

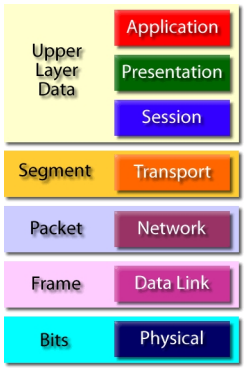
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU) :

Protocol Data Unit - PDU



The following answers are incorrect:

Data – Application layer PDU

Segment – Transport layer PDU

Frame/bit – LAN or WAN interface layer PDU

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 page number 272

Question 2372

Which of the following is a characteristic of timebox management?

- ☐ Not suitable for prototyping or rapid application development (RAD)
- ☐ Eliminates the need for a quality process
- ☒ Prevents cost overruns and delivery delays
- ☐ Separates system and user acceptance testing

Explanation:

Explanation:

Timebox management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

Question 2373

Which of the following is the BEST method to defend against social engineering attacks?

- ☐ Periodically perform antivirus scans to identify malware.
- ☐ Communicate guidelines to limit information posted to public sites.
- ☐ Monitor for unauthorized access attempts and failed logins.
- ☒ Employ the use of a web-content filtering solution.

Question 2374

Which of the following access rights in the production environment should be granted to a developer to maintain segregation of duties?

- ☐ Database administration
- ☐ Emergency support
- ☐ IT operations
- ☒ System administration

Question 2375

The MAJOR advantage of a component-based development approach is the:

- ☐ ability to manage an unrestricted variety of data types.
- ☐ provision for modeling complex relationships.
- ☐ capacity to meet the demands of a changing environment.
- ☒ support of multiple development environments.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not the most significant advantages of a component-based development approach.

Question 2376

Which of the following are often considered as the first defensive line in protecting a typical data and information environment?

- ☐ certificates
- ☐ security token
- ☒ password
- ☐ biometrics
- ☐ None of the choices.

Explanation:

Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password.

Question 2377

What should be a security manager's PRIMARY objective in the event of a security incident?

- ☐ Identify the source of the breach and how it was perpetrated.
- ☒ Contain the threat and restore operations in a timely manner.
- ☐ Ensure that normal operations are not disrupted.
- ☐ Identify lapses in operational control effectiveness.

Question 2378

Which of the following statement INCORRECTLY describes circuit switching technique?

- ☒ Packet uses many different dynamic paths to get the same destination
- ☐ Connection oriented virtual links
- ☐ Fixed delays
- ☐ Traffic travels in a predictable and constant manner

Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about circuit switching.

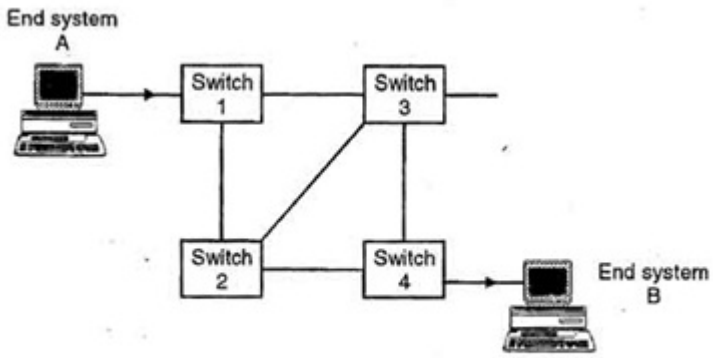
Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below information about WAN message transmission technique:

Message Switching

Message switching is a network switching technique in which data is routed in its entirety from the source node to the destination node, one hope at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, the message-switched network stores and delays the message until ample resources become available for effective transmission of the message.

Message Switching



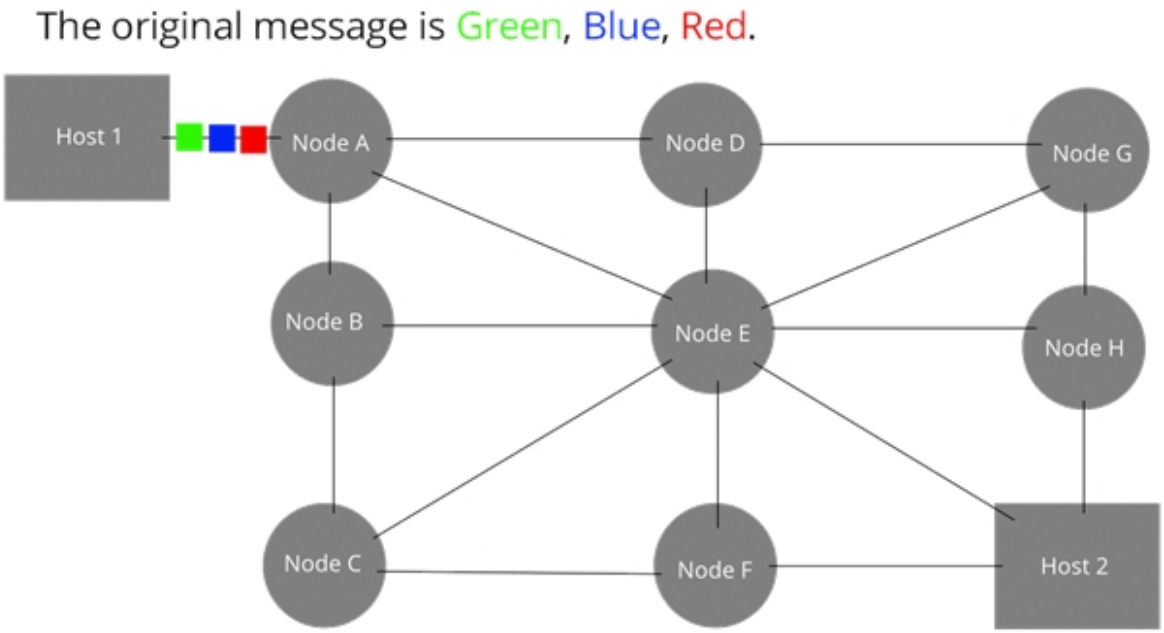
Message switched data network

Packet Switching

Refers to protocols in which messages are divided into packets before they are sent. Each packet is then transmitted individually and can even follow different routes to its destination. Once all the packets forming a message arrive at the destination, they are recompiled into the original message.

Packet Switching

Licensed to Berend Post berend.post@it-university.nl



Circuit Switching

Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate.

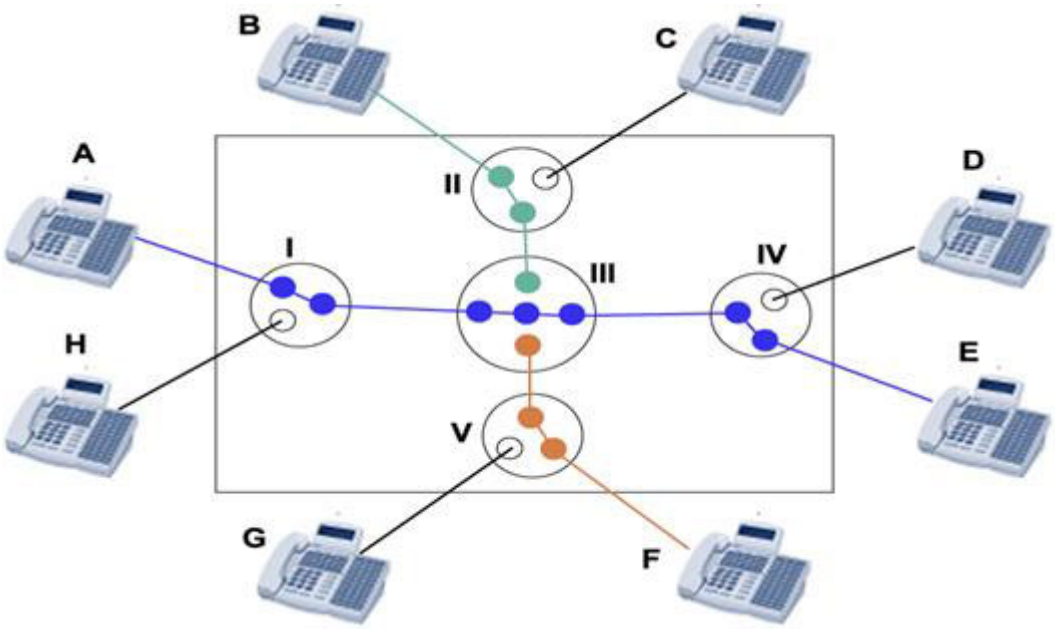
The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.

In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.

Circuit Switching

Licensed to Berend Post berend.post@it-university.nl



See a table below comparing Circuit Switched versus Packet Switched networks:

Difference between Circuit and packet switching

	Circuit Switching	Packet Switching
Dedicated "copper" path	Yes	No
Bandwidth available	Fixed	Dynamic
Potentially wasted bandwidth	Yes	No
Store-and-forward-transmission	No	Yes
Each packet follows the same route	Yes	No
Call setup	Required	Not required
When can congestion occur	At setup time	On every packet
Charging	Per minute	Per packet

Virtual circuit

In telecommunications and computer networks, a virtual circuit (VC), synonymous with virtual connection and virtual channel, is a connection oriented communication service that is delivered by means of packet mode communication.

After a connection or virtual circuit is established between two nodes or application processes, a bit stream or byte stream may be delivered between the nodes; a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames.

Licensed to Berend Post berend.post@it-university.nl

Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection establishment phase. However, circuit switching provides constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as:

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

varying load from other users sharing the same network resources by means of statistical multiplexing, etc.

The following were incorrect answers:

The other options presented correctly describes about circuit switching.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 265

Question 2379

An organization wants to test business continuity using a scenario in which there are many remote workers trying to access production data at the same time. Which of the following is the BEST testing method in this situation?

- ☐ Application failover testing.
- ☒ Network stress testing.
- ☐ Alternate site testing.
- ☐ Network penetration testing.

Question 2380

Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

- ☐ The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
- ☐ All personal SET certificates are stored securely in the buyer's computer.
- ☒ The buyer is liable for any transaction involving his/her personal SET certificates.
- ☐ The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of their personal SET certificates for e- commerce transactions. Depending upon the agreement between the merchant and the buyer's credit card issuer, the merchant will have access to the credit card number and expiration date. Secure data storage in the buyer's computer (local computer security) is not part of the SET standard.

Although the buyer is not required to enter their credit card data, they will have to handle the wallet software.

Question 2381

Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?

- ☐ Data backups are performed on a timely basis
- ☐ A recovery site is contracted for and available as needed
- ☒ Human safety procedures are in place
- ☐ insurance coverage is adequate and premiums are current

Explanation:

Explanation:

The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.

Question 2382

When conducting a post-implementation review, which of the following is the BEST way to determine whether the value from an IT project has been achieved?

- ☐ Calculate the return on investment (ROI).
- ☐ Interview stakeholders.
- ☒ Conduct an earned value analysis (EVA).
- ☐ Survey end users.

Question 2383

A database is denormalized in order to:

- ☐ prevent loss of data.
- ☒ increase processing efficiency.
- ☐ ensure data integrity.
- ☐ save storage space.

Licensed to Berend Post berend.post@it-university.nl

Question 2384

Which of the following is the MOST important consideration when designing information security architecture?

- ☐ Risk management parameters for the organization are defined.
- ☐ The existing threat landscape is monitored.
- ☐ The information security architecture is aligned with industry standards.
- ☒ The level of security supported is based on business decisions.

Question 2385

When reviewing the process by which a contract for the outsourcing of various IT functions was completed, an IS auditor would ensure that the successful contractor:

- ☐ has eliminated the risks of outsourcing.
- ☒ maintains an internal audit function.
- ☐ requires a confidentiality agreement to be signed by all employees.
- ☐ was selected according to established business criteria.

Question 2386

Which of the following is the BEST way to mitigate the risk of unintentional modifications associated with complex calculations in end-user computing (EUC)?

- ☐ Verify EUC results through manual calculations.
- ☐ Operate copies of EUC programs out of a secure library.
- ☒ Implement data integrity checks.
- ☐ Utilize an independent party to review the source calculations.

Question 2387

An IS auditor is evaluating the access controls at a multinational company with a shared network infrastructure. Which of the following is MOST important?

- ☐ Simplicity of end-to-end communication paths
- ☐ Remote network administration
- ☒ Common security policies
- ☐ Logging of network information at user level

Licensed to Berend Post berend.post@it-university.nl

Question 2388

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- ☒ allow changes, which will be completed using after-the-fact follow-up.
- ☐ allow undocumented changes directly to the production library.
- ☐ do not allow any emergency changes.
- ☐ allow programmers permanent access to production programs.

Explanation:

Explanation:

There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should be completed using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

Question 2389

As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains small enhancements and fixes?

- ☐ Major software Release
- ☒ Minor software Release
- ☐ Emergency software release
- ☐ General software Release

Explanation:

Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner. Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release

 Licensed to Berend Post berend.post@it-university.nl

Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Software Release management is a process through which software is made available to user. Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release – Not a valid type of software release.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 244

Licensed to Berend Post berend.post@it-university.nl

Question 2390

What should an IS auditor do when informed that some recommendations cannot be implemented due to financial constraints?

- ☒ Document management's response in the working papers.
- ☐ Insist the recommendations be implemented.
- ☐ Agree to waive the recommendations.
- ☐ Suggest management identify cost-effective alternatives.

Question 2391

The PRIMARY objective of implementing corporate governance by an organization's management is to:

- ☒ provide strategic direction.
- ☐ control business operations.
- ☐ align IT with business.
- ☐ implement best practices.

Explanation:

Explanation:

Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence, the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

Question 2392

The purpose of code signing is to provide assurance that:

- ☒ the software has not been subsequently modified.
- ☐ the application can safely interface with another signed application.
- ☐ the signer of the application is trusted.
- ☐ the private key of the signer has not been compromised.

Explanation:

Explanation:

Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

Licensed to Berend Post berend.post@it-university.nl

Question 2393

An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

- ☐ the controls already in place.
- ☐ the effectiveness of the controls in place.
- ☐ the mechanism for monitoring the risks related to the assets.
- ☒ the threats/vulnerabilities affecting the assets.

Explanation:

Explanation:

One of the key factors to be considered while assessing the risks related to the use of various information systems is the threats and vulnerabilities affecting the assets. The risks related to the use of information assets should be evaluated in isolation from the installed controls. Similarly, the effectiveness of the controls should be considered during the risk mitigation stage and not during the risk assessment phase A mechanism to continuously monitor the risks related to assets should be put in place during the risk monitoring function that follows the risk assessment phase.

Question 2394

A company uses a standard form to document and approve all changes in production programs. To ensure that the forms are properly authorized, which of the following is the MOST effective sampling method?

- ☐ Attribute
- ☐ Variable
- ☒ Discovery
- ☐ Monetary

Question 2395

Which of the following components of a scheduling tool BEST prevents job failures due to insufficient system resources?

- ☐ Job dependencies
- ☐ Delayed job starts
- ☒ Exception handling
- ☐ Error alerts

Licensed to Berend Post berend.post@it-university.nl

Question 2396

Which of the following BEST minimizes performance degradation of servers used to authenticate users of an e-commerce website?

☐ Configure each authentication server and ensure that the disks of each server form part of a duplex.
☒ Configure each authentication server as belonging to a cluster of authentication servers.
☐ Configure a single server as a primary authentication server and a second server as a secondary authentication server.
☐ Configure each authentication server and ensure that each disk of its RAID is attached to the primary controller.

Question 2397

Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

☒ Alternative routing
☐ Diverse routing
☐ Long haul network diversity
☐ Last mile circuit protection

Explanation:

Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

Licensed to Berend Post berend.post@it-university.nl

Question 2398

A bank is selecting a server for its retail accounts application. To ensure that the server can handle a high volume of transactions with the required response times, which test should the IS auditor recommend?

- ☐ Regression
- ☐ Acceptance
- ☒ Benchmark
- ☐ Integration

Question 2399

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- ☐ Report that the organization does not have effective project management.
- ☐ Recommend the project manager be changed.
- ☐ Review the IT governance structure.
- ☒ Review the conduct of the project and the business case.

Explanation:

Explanation:

Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound IT governance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

Question 2400

Processing controls ensure that data is accurate and complete, and is processed only through which of the following?

- ☐ Documented routines
- ☒ Authorized routines
- ☐ Accepted routines
- ☐ Approved routines

Explanation:

Explanation:

Processing controls ensure that data is accurate and complete, and is processed only through authorized routines.

Licensed to Berend Post berend.post@it-university.nl

Question 2401

Which of the following is MOST important to include in an organization's incident response plan to help prevent similar incidents from happening in the future?

- ☐ Documentation of incident details
- ☐ Incident closure procedures
- ☐ Containment and neutralization actions
- ☒ Post-incident review

Question 2402

Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource?

- ☐ Systems logs
- ☒ Access control lists (ACL)
- ☐ Application logs
- ☐ Error logs

Explanation:

Explanation:

IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

Question 2403

The MAIN purpose of a transaction audit trail is to:

- ☐ reduce the use of storage media.
- ☒ determine accountability and responsibility for processed transactions.
- ☐ help an IS auditor trace transactions.
- ☐ provide useful information for capacity planning.

Explanation:

Explanation:

Enabling audit trails aids in establishing the accountability and responsibility for processed transactions by tracing them through the information system. Enabling audit trails increases the use of disk space. A transaction log file would be used to trace transactions, but would not aid in determining accountability and responsibility. The objective of capacity planning is the efficient and effective use of IT resources and requires information such as CPU utilization, bandwidth, number of users, etc.

Licensed to Berend Post berend.post@it-university.nl

Question 2404

Which of the following is a passive attack to a network?

- ☐ Message modification
- ☐ Masquerading
- ☐ Denial of service
- ☒ Traffic analysis

Explanation:

Explanation:

The intruder determines the nature of the flow of traffic (traffic analysis) between defined hosts and is able to guess the type of communication taking place. Message modification involves the capturing of a message and making unauthorized changes or deletions, changing the sequence or delaying transmission of captured messages. Masquerading is an active attack in which the intruder presents an identity other than the original identity. Denial of service occurs when a computer connected to the internet is flooded with data and/or requests that must be processed.

Question 2405

An organization's software develops need access to personally identifiable information (PII) stored in a particular data format. Which of the following would be the BEST way to protect this sensitive information while allowing the developers to use it in development and test environments?

- ☐ Data masking
- ☐ Data encryption
- ☒ Data tokenization
- ☐ Data abstraction

Question 2406

Which of the following is the MOST effective method of destroying sensitive data stored on electronic media?

- ☒ Physical destruction
- ☐ Degaussing
- ☐ Random character overwrite
- ☐ Low-level formatting

Explanation:

Reference: https://www.isaca.org/Journal/archives/2010/Volume-6/Pages/An-Introduction-to-Digital-Records-Management.aspx

Licensed to Berend Post berend.post@it-university.nl

Question 2407

In which of the following database model is the data organized into a tree-like structure, implying a single parent for each record?

- ☒ Hierarchical database model
- ☐ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Explanation:

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

Hierarchical database model

Network model

Relational model

Object-relational database models

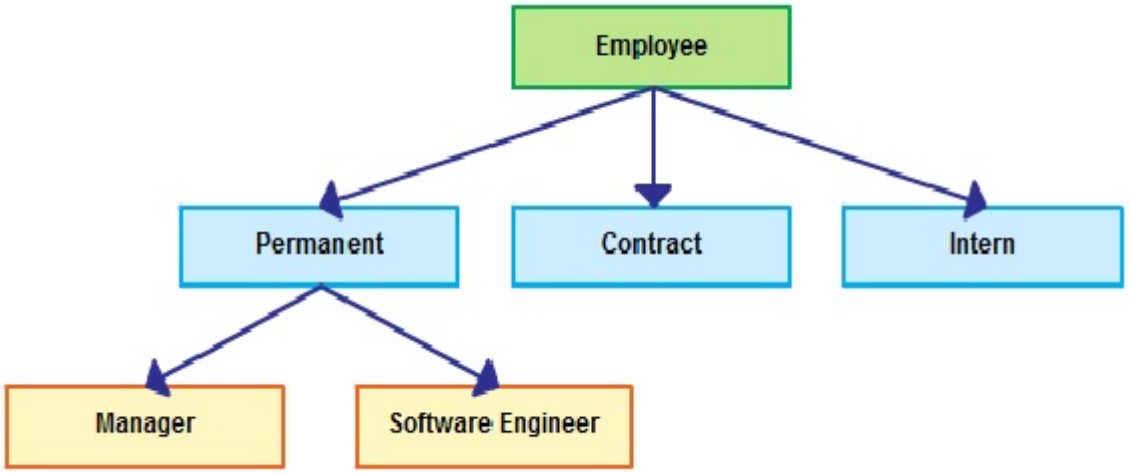
Hierarchical database model

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order. Hierarchical structures were widely used in the early mainframe database management systems, such as the Information Management System (IMS) by IBM, and now describe the structure of XML documents. This structure allows one one-to-many relationship between two types of data. This structure is very efficient to describe many relationships in the real world; recipes, table of contents, ordering of paragraphs/verses, any nested and sorted information.

This hierarchy is used as the physical order of records in storage. Record access is done by navigating through the data structure using pointers combined with sequential accessing. Because of this, the hierarchical structure is inefficient for certain database operations when a full path (as opposed to upward link and sort field) is not also included for each record. Such limitations have been compensated for in later IMS versions by additional logical hierarchies imposed on the base physical hierarchy.

Licensed to Berend Post berend.post@it-university.nl

Hierarchical database model



Network database model

The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents. It was the most popular before being replaced by the relational model, and is defined by the CODASYL specification.

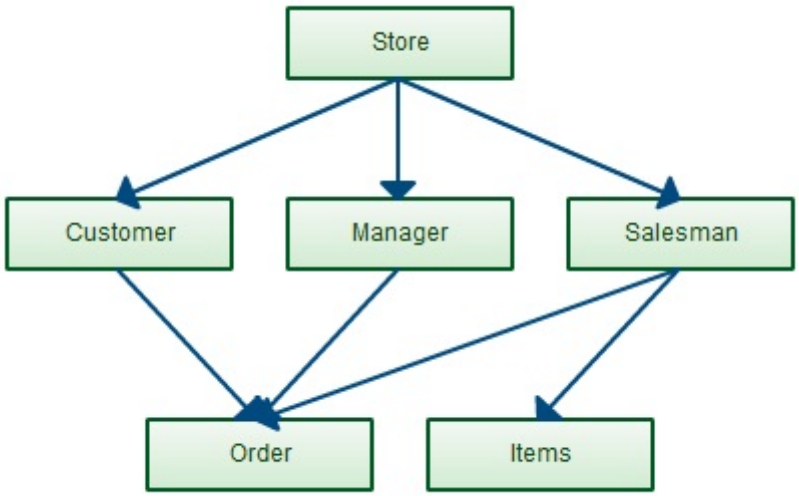
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

A set consists of circular linked lists where one record type, the set owner or parent, appears once in each circle, and a second record type, the subordinate or child, may appear multiple times in each circle. In this way a hierarchy may be established between any two record types, e.g., type A is the owner of B. At the same time another set may be defined where B is the owner of A. Thus all the sets comprise a general directed graph (ownership defines a direction), or network construct. Access to records is either sequential (usually in each record type) or by navigation in the circular linked lists.

The network model is able to represent redundancy in data more efficiently than in the hierarchical model, and there can be more than one path from an ancestor node to a descendant. The operations of the network model are navigational in style: a program maintains a current position, and navigates from one record to another by following the relationships in which the record participates. Records can also be located by supplying key values.

Network Database model

Licensed to Berend Post berend.post@it-university.nl



Relational database model

In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database.

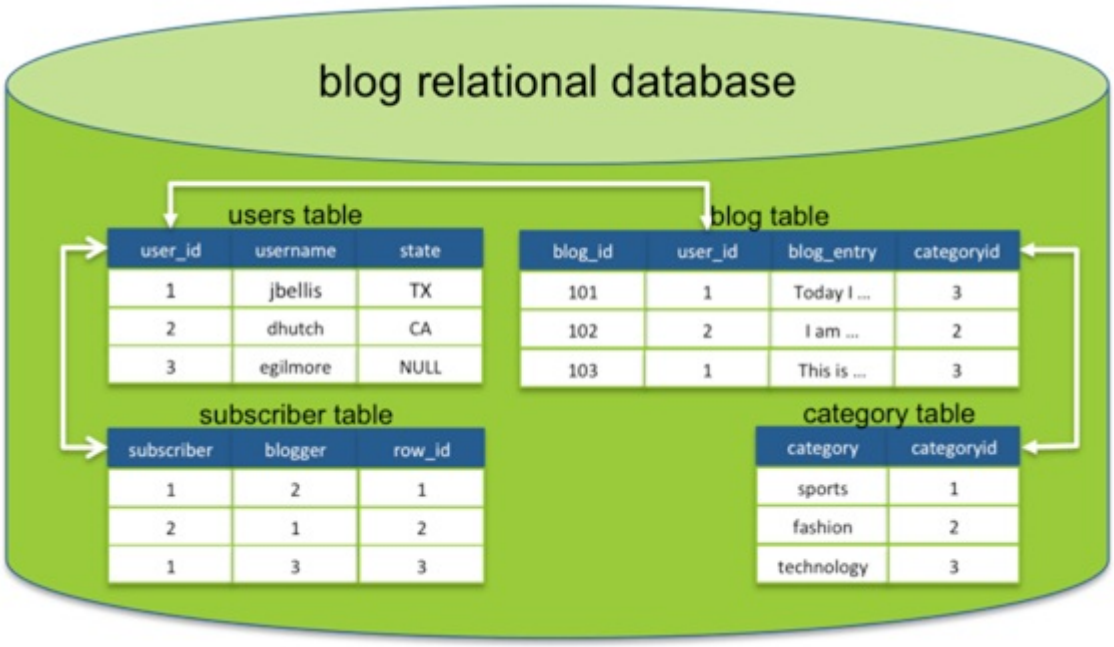
In the relational model, related records are linked together with a "key".

The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want from it, and let the database management system software take care of describing data structures for storing the data and retrieval procedures for answering queries.

Most relational databases use the SQL data definition and query language; these systems implement what can be regarded as an engineering approximation to the relational model. A table in an SQL database schema corresponds to a predicate variable; the contents of a table to a relation; key constraints, other constraints, and SQL queries correspond to predicates. However, SQL databases, including DB2, deviate from the relational model in many details, and Cod fiercely argued against deviations that compromise the original principles.

Relational database model

Licensed to Berend Post berend.post@it-university.nl



Object-relational database Model

An object-relational database (ORD), or object-relational database management system (ORDBMS), is a database management system (DBMS) similar to a relational database, but with an object-oriented database model: objects, classes and inheritance are directly supported in database schemas and in the query language. In addition, just as with pure relational systems, it supports extension of the data model with custom data-types and methods.

Example of an object-oriented database model

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Network model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

Relational model- In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database

 Licensed to Berend Post berend.post@it-university.nl

and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 254

Question 2408

When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

- ☒ hardware is protected against power surges.
- ☐ integrity is maintained if the main power is interrupted.
- ☐ immediate power will be available if the main power is lost.
- ☐ hardware is protected against long-term power fluctuations.

Explanation:

Explanation:

A voltage regulator protects against short-term power fluctuations. It normally does not protect against long-term surges, nor does it maintain the integrity if power is interrupted or lost.

Question 2409

Which of the following provides for the GREATEST cost reduction in a large data center?

- ☒ Server consolidation
- ☐ Staff rotation
- ☐ Power conditioning
- ☐ Job-scheduling software

Question 2410

An organization is developing data classification standards and has asked internal audit for advice on aligning the standards with best practices. Internal audit would MOST likely recommend the standards should be:

- ☐ based on the results of an organization-wide risk assessment.
- ☐ based on the business requirements for confidentiality of the information.
- ☒ aligned with the organization's segregation of duties requirements.
- ☐ based on the business requirements for authentication of the information.

Licensed to Berend Post berend.post@it-university.nl

Question 2411

An information systems security officer's PRIMARY responsibility for business process applications is to:

- ☐ create role-based rules for each business process.
- ☒ ensure access rules agree with policies.
- ☐ authorize secured emergency access.
- ☐ approve the organization's security policy.

Question 2412

Which of the following would BEST describe an audit risk?

- ☐ The company is being sued for false accusations.
- ☒ The financial report may contain undetected material errors.
- ☐ Key employees have not taken vacation for 2 years.
- ☐ Employees have been misappropriating funds.

Question 2413

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

- ☐ test data covering critical applications.
- ☐ detailed test plans.
- ☐ quality assurance test specifications.
- ☒ user acceptance testing specifications

Explanation:

Explanation: A key objective in any software development project is to ensure that the developed software will meet the business objectives and the requirements of the user. The users should be involved in the requirements definition phase of a development project and user acceptance test specification should be developed during this phase. The other choices are generally performed during the system testing phase.

Question 2414

Which of the following is the GREATEST concern associated with control self-assessments?

- ☐ Employees may have insufficient awareness of controls
- ☒ Controls may not be assessed objectively
- ☐ Communication between operational management and senior management may not be effective
- ☐ The assessment may not provide sufficient assurance to stakeholders

Licensed to Berend Post berend.post@it-university.nl

Question 2415

Which of the following outsourced services has the GREATEST need for security monitoring?

- ☐ Web site hosting
- ☐ Application development
- ☐ Virtual private network (VPN) services
- ☒ Enterprise infrastructure

Question 2416

An organization is considering moving one of its critical business applications to a cloud hosting service. The cloud provider may not provide the same level of security for this application as the organization. Which of the following will provide the BEST information to help maintain the security posture?

- ☒ Risk assessment
- ☐ Cloud security strategy
- ☐ Vulnerability assessment
- ☐ Risk governance framework

Question 2417

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- ☒ a clear business case has been approved by management.
- ☐ corporate security standards will be met.
- ☐ users will be involved in the implementation plan.
- ☐ the new system will meet all required user functionality.

Explanation:

Explanation:

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditor's first concern.

Licensed to Berend Post berend.post@it-university.nl

Question 2418

Which of the following fourth generation language is a development tools to generate lower level programming languages?

- ☐ Query and report generator
- ☐ Embedded database 4GLs
- ☐ Relational database 4GL
- ☒ Application generators

Explanation:

Application generators - These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.

For CISA exam you should know below mentioned types of 4GLs

Query and report generator – These specialize language can extract and produce reports. Recently more powerful language has been produced that can access database records, produce complex on-line output and be developed in an almost natural language.

Embedded database 4GLs – These depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line. These allow the application developer to make better use of DBMS product, but they often are not end-user-oriented. Example include SQL+ MANTIS and NATURAL.

Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.

The following were incorrect answers:

Query and report generator – These specialize language can extract and produce reports.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line.

Licensed to Berend Post berend.post@it-university.nl

Embedded database 4GLs – These depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 209

Question 2419

Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?

- ☐ A report on the maturity of controls
- ☐ Up-to-date policy and procedures documentation
- ☐ Existence of an industry-accepted framework
- ☒ Results of an independent assessment

Question 2420

Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

- ☒ physically separated from the data center and not subject to the same risks.
- ☐ given the same level of protection as that of the computer data center.
- ☐ outsourced to a reliable third party.
- ☐ equipped with surveillance capabilities.

Explanation:

Explanation:

It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

Licensed to Berend Post berend.post@it-university.nl

Question 2421

Which of the following software development methodology is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☒ Component based development

Explanation:

Component-based software engineering (CBSE) (also known as component-based development (CBD)) is a branch of software engineering that emphasizes the separation of concerns in respect of the wide-ranging functionality available throughout a given software system. It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

Software engineers[who?] regard components as part of the starting platform for service-orientation. Components play this role, for example, in web services, and more recently, in service-oriented architectures (SOA), whereby a component is converted by the web service into a service and subsequently inherits further characteristics beyond that of an ordinary component.

Components can produce or consume events and can be used for event-driven architectures (EDA).

Definition and characteristics of components

An individual software component is a software package, a web service, a web resource, or a module that encapsulates a set of related functions (or data).

All system processes are placed into separate components so that all of the data and functions inside each component are semantically related (just as with the contents of classes). Because of this principle, it is often said that components are modular and cohesive.

With regard to system-wide co-ordination, components communicate with each other via interfaces. When a component offers services to the rest of the system, it adopts a provided interface that specifies the services that other components can utilize, and how they can do so. This interface can be seen as a signature of the component - the client does not need to know about the inner workings of the component (implementation) in order to make use of it. This principle results in components referred to as encapsulated. The UML illustrations within this article represent provided interfaces by a lollipop-symbol attached to the outer edge of the component.

Licensed to Berend Post berend.post@it-university.nl

However, when a component needs to use another component in order to function, it adopts a used interface that specifies the services that it needs. In the UML illustrations in this article, used interfaces are represented by an open socket symbol attached to the outer edge of the component.

A simple example of several software components - pictured within a hypothetical holiday-reservation system represented in UML 2.0.

Another important attribute of components is that they are substitutable, so that a component can replace another (at design time or run-time), if the successor component meets the requirements of the initial component (expressed via the interfaces). Consequently, components can be replaced with either an updated version or an alternative without breaking the system in which the component operates.

As a general rule of thumb for engineers substituting components, component B can immediately replace component A, if component B provides at least what component A provided and uses no more than what component A used.

Software components often take the form of objects (not classes) or collections of objects (from object-oriented programming), in some binary or textual form, adhering to some interface description language (IDL) so that the component may exist autonomously from other components in a computer.

When a component is to be accessed or shared across execution contexts or network links, techniques such as serialization or marshalling are often employed to deliver the component to its destination.

Reusability is an important characteristic of a high-quality software component. Programmers should design and implement software components in such a way that many different programs can reuse them. Furthermore, component-based usability testing should be considered when software components directly interact with users.

It takes significant effort and awareness to write a software component that is effectively reusable. The component needs to be:

fully documented

thoroughly tested

robust - with comprehensive input-validity checking

Licensed to Berend Post berend.post@it-university.nl

able to pass back appropriate error messages or return codes

designed with an awareness that it will be put to unforeseen uses

The following were incorrect answers:

Agile Development - Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 194

Question 2422

Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

- ☒ Computation speed
- ☐ Ability to support digital signatures
- ☐ Simpler key distribution
- ☐ Greater strength for a given key length

Explanation:

Explanation:

The main advantage of elliptic curve encryption over RSA encryption is its computation speed. This method was first independently suggested by Neal Koblitz and Victor S. Miller. Both encryption methods support digital signatures and are used for public key encryption and distribution. However, a stronger key per se does not necessarily guarantee better performance, but rather the actual algorithm employed.

 Licensed to Berend Post berend.post@it-university.nl

Question 2423

When auditing a disaster recovery plan for a critical business area, an IS auditor finds that it does not cover all the systems. Which of the following is the MOST appropriate action for the IS auditor?

- ☒ Alert management and evaluate the impact of not covering all systems.
- ☐ Cancel the audit.
- ☐ Complete the audit of the systems covered by the existing disaster recovery plan.
- ☐ Postpone the audit until the systems are added to the disaster recovery plan.

Explanation:

Explanation:

An IS auditor should make management aware that some systems are omitted from the disaster recovery plan. An IS auditor should continue the audit and include an evaluation of the impact of not including all systems in the disaster recovery plan. Cancelling the audit, ignoring the fact that some systems are not covered or postponing the audit are inappropriate actions to take.

Question 2424

Batch control reconciliation is a _____ (fill the blank) control for mitigating risk of inadequate segregation of duties.

- ☐ Detective
- ☐ Corrective
- ☐ Preventative
- ☒ Compensatory

Explanation:

Explanation:

Batch control reconciliations is a compensatory control for mitigating risk of inadequate segregation of duties.

Question 2425

Which of the following is the BEST approach to make strategic information security decisions?

- ☐ Establish regular information security status reporting
- ☐ Establish business unit security working groups
- ☐ Establish periodic senior management meetings
- ☒ Establish an information security steering committee

Licensed to Berend Post berend.post@it-university.nl

Question 2426

The MOST effective biometric control system is the one:

- ☐ which has the highest equal-error rate (EER).
- ☒ which has the lowest EER.
- ☐ for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- ☐ for which the FRR is equal to the failure-to-enroll rate (FER).

Explanation:

Explanation:

The equal-error rate (EER) of a biometric system denotes the percent at which the false- acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

Question 2427

A start-up company acquiring servers for its order-taking system is unable to predict the volume of transactions. Which of the following is MOST important for the company to consider?

- ☒ Scalability
- ☐ Configuration
- ☐ Optimization
- ☐ Compatibility

Question 2428

Which of the following is NOT an example of corrective control?

- ☐ OS Upgrade
- ☐ Backup and restore
- ☐ Contingency planning
- ☒ System Monitoring

Explanation:

Explanation:

The word NOT is used as a keyword in the question. You need to find out a security control from given options which in not corrective control. System Monitoring is a detective control and not a corrective control.

For your exam you should know below information about different security controls

Licensed to Berend Post berend.post@it-university.nl

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to

find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other

technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the

 Licensed to Berend Post berend.post@it-university.nl

authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective

nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security

incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take

many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default

 Licensed to Berend Post berend.post@it-university.nl

administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

 Licensed to Berend Post berend.post@it-university.nl

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device

Licensed to Berend Post berend.post@it-university.nl

provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples belong to corrective control.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Licensed to Berend Post berend.post@it-university.nl

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 2429

Which of the following IS audit findings should be of GREATEST concern when preparing to migrate to a new core system using a direct cut-over?

- ☐ Incomplete test cases for some critical reports
- ☐ Informal management approval to go live
- ☒ Lack of a rollback strategy for the system go-live
- ☐ Plans to use some workarounds for an extended period after go-live

Question 2430

When an intrusion into an organization's network is detected, which of the following should be performed FIRST?

- ☐ Block all compromised network nodes.
- ☐ Protect information in the compromised systems.
- ☒ Develop a response to the incident.
- ☐ Identify nodes that have been compromised.

Question 2431

In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

- ☒ Appliances
- ☐ Operating system-based
- ☐ Host-based
- ☐ Demilitarized

Explanation:

Explanation:

The software for appliances is embedded into chips. Firmware-based firewall products cannot be moved to higher capacity servers. Firewall software that sits on an operating system can always be scalable due to its ability to enhance the power of servers. Host- based firewalls operate on top of the server operating system and are scalable. A demilitarized zone is a model of firewall implementation and is not a firewall architecture.

Licensed to Berend Post berend.post@it-university.nl

Question 2432

Which of the following is NOT a component of IPSec?

- ☐ Authentication Header
- ☐ Encapsulating Security Payload
- ☒ Key Distribution Center
- ☐ Internet Key Exchange

Explanation:

AH, ESP and IKE are the three main components of IPSec. A KDC (Key Distribution Center) is a component of Kerberos, not IPSec.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 217).

Question 2433

Which of the following component of an expert system enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☒ Data interface

Explanation:

Data Interface enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

For CISA Exam you should know below information about Artificial Intelligence and Expert System

Artificial intelligence is the study and application of the principles by which:

Knowledge is acquired and used

Goals are generated and achieved

Information is communicated

Collaboration is achieved

Concepts are formed

Languages are developed

Two main programming languages that have been developed for artificial intelligence are LISP and PROLOG.

Licensed to Berend Post berend.post@it-university.nl

Expert system are compromised primary components, called shells, when they are not populated with particular data, and the shells are designed to host new expert system.

Keys to the system is the knowledge base (KB), which contains specific information or fact patterns associated with a particular subject matter and the rule for interpreting these facts. The KB interface with a database in obtaining data to analyze a particular problem in deriving an expert conclusion. The information in the KB can be expressed in several ways:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule – Expressing declarative knowledge through the use of if-then relationships. For example, if a patient's body temperature is over 39 degrees Celsius and their pulse is under 60, then they might be suffering from a certain disease.

Semantic nets – Consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes. Semantic nets resemble a data flow diagram and make use of an inheritance mechanism to prevent duplication of a data.

Additionally, the inference engine shown is a program that uses the KB and determines the most appropriate outcome based on the information supplied by the user. In addition, an expert system includes the following components

Knowledge interface – Allows the expert to enter knowledge into the system without the traditional mediation of a software engineer.

Data Interface – Enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

The following were incorrect answers:

Decision Tree – Using questionnaires to lead the user through a series of choices, until a conclusion is reached. Flexibility is compromised because the user must answer the questions in an exact sequence.

Rule - Expressing declarative knowledge through the use of if-then relationships.

Licensed to Berend Post berend.post@it-university.nl

Semantic nets - Semantic nets consist of a graph in which the node represent physical or conceptual object and the arcs describe the relationship between the nodes.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 187

Question 2434

During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could user to force authorization step before authentication?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☒ Race Condition

Explanation:

A race condition is when processes carry out their tasks on a shared resource in an incorrect order. A race condition is possible when two or more processes use a shared resource, as in data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result will be much different than if process1 carried out its tasks on the data before process 2.

In software, when the authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the authorization step to be completed before the authentication step. This would be a flaw in the software that the attacker has figured out how to exploit. A race condition occurs when two or more processes use the same resource and the sequences of steps within the software can be carried out in an improper order, something that can drastically affect the output. So, an attacker can force the authorization step to take place before the authentication step and gain unauthorized access to a resource.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Licensed to Berend Post berend.post@it-university.nl

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

Masquerading - A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack. Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process. The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network. The amount of access masquerade attackers get depends on the level of authorization they've managed to attain. As such, masquerade attackers can have a full smorgasbord of cyber crime opportunities if they've gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 324

Official ISC2 guide to CISSP CBK 3rd Edition Page number 66

CISSP All-In-One Exam guide 6th Edition Page Number 161

Question 2435

Which of the following refers to the collection of policies and procedures for implementing controls capable of restricting access to computer software and data files?

- ☐ Binary access control
- ☐ System-level access control
- ☒ Logical access control
- ☐ Physical access control
- ☐ Component access control
- ☐ None of the choices.

Explanation:

Explanation:

Logical access control is about the use of a collection of policies, procedures, and controls to restrict access to computer software and data files.

Such control system should provide reasonable assurance that an organization's objectives are being properly achieved securely and reliably.

Licensed to Berend Post berend.post@it-university.nl

Question 2436

Which of the following is the MOST effective control for a utility program?

- ☐ Renaming the versions in the programmers' libraries
- ☐ Installing the program on a separate server
- ☐ Storing the program in a production library
- ☒ Allowing only authorized personnel to use the program

Question 2437

An IS auditor has been asked to perform a post-implementation assessment of a new corporate human resources (HR) system. Which of the following control areas would be MOST important to review for the protection of employee information?

- ☐ Logging capabilities
- ☒ Authentication mechanisms
- ☐ Data retention practices
- ☐ System architecture

Question 2438

Which of the following is the BEST way to address ongoing concerns with the quality and accuracy of internal audits?

- ☒ Engage an independent review of the audit function.
- ☐ Require peer reviews of audit workpapers.
- ☐ Implement performance management for IS auditors.
- ☐ Require IS audit management to lead exit meetings.

Question 2439

Which of the following audit risk is related to material error exist that would not be prevented or detected on timely basis by the system of internal controls?

- ☐ Inherent Risk
- ☒ Control Risk
- ☐ Detection Risk
- ☐ Overall Audit Risk

Explanation:

Explanation:

The risk that material error exist that would not be prevented or detected on timely basis by the system of internal controls. For example, the control risk associated with manual review could be

Licensed to Berend Post berend.post@it-university.nl

high because activities requiring investigation are often easily missed due to the volume of logged information.

For your exam you should know below information about audit risk:

Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR), and can be calculated thus:

AR = IR • CR • DR

Inherent Risk

Auditors must determine risks when working with clients. One type of risk to be aware of is inherent risk. While assessing this level of risk, you ignore whether the client has internal controls in place (such as a secondary review of financial statements) in order to help mitigate the inherent risk. You consider the strength of the internal controls when assessing the client's control risk. Your job when assessing inherent risk is to evaluate how susceptible the financial statement assertions are to material misstatement given the nature of the client's business. A few key factors can increase inherent risk.

Environment and external factors: Here are some examples of environment and external factors that can lead to high inherent risk:

Rapid change: A business whose inventory becomes obsolete quickly experiences high inherent risk.

Expiring patents: Any business in the pharmaceutical industry also has inherently risky environment and external factors. Drug patents eventually expire, which means the company faces competition from other manufacturers marketing the same drug under a generic label.

State of the economy: The general level of economic growth is another external factor affecting all businesses.

Availability of financing: Another external factor is interest rates and the associated availability of financing. If your client is having problems meeting its short-term cash payments, available loans with low interest rates may mean the difference between your client staying in business or having to close its doors.

Prior-period misstatements: If a company has made mistakes in prior years that weren't material (meaning they weren't significant enough to have to change), those errors still exist in the financial statements. You have to aggregate prior-period misstatements with current year misstatements to see if you need to ask the client to adjust the account for the total misstatement.

Licensed to Berend Post berend.post@it-university.nl

You may think an understatement in one year compensates for an overstatement in another year. In auditing, this assumption isn't true. Say you work a cash register and one night the register comes up $20 short. The next week, you somehow came up $20 over my draw count. The $20 differences are added together to represent the total amount of your mistakes which is $40 and not zero. Zero would indicate no mistakes at all had occurred.

Susceptibility to theft or fraud: If a certain asset is susceptible to theft or fraud, the account or balance level may be considered inherently risky. For example, if a client has a lot of customers who pay in cash, the balance sheet cash account is going to have risk associated with theft or fraud because of the fact that cash is more easily diverted than customer checks or credit card payments.

Looking at industry statistics relating to inventory theft, you may also decide to consider the inventory account as inherently risky. Small inventory items can further increase the risk of this account valuation being incorrect because those items are easier to conceal (and therefore easier to steal).

Control Risk

Control risk has been defined under International Standards of Auditing (ISAs) as following:

The risk that a misstatement that could occur in an assertion about a class of transaction, account balance or disclosure and that could be material, either individually or when aggregated with other misstatements, will not be prevented, or detected and corrected, on a timely basis by the entity's internal control.

In simple words control risk is the probability that a material misstatement exists in an assertion because that misstatement was not either prevented from entering entity's financial information or it was not detected and corrected by the internal control system of the entity.

It is the responsibility of the management and those charged with governance to implement internal control system and maintain it appropriately which includes managing control risk.

There can be many reasons for control risk to arise and why it cannot be eliminated absolutely. But some of them are as follows:

Cost-benefit constraints

Circumvention of controls

Inappropriate design of controls

Licensed to Berend Post berend.post@it-university.nl

Inappropriate application of controls

Lack of control environment and accountability

Novel situations

Outdated controls

Inappropriate segregation of duties

Detection Risk

Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements.

An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions.

Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

The following answers are incorrect:

Inherent Risk - It is the risk level or exposure of a process or entity to be audited without taking into account the control that management has implemented.

Detection risk - The risk that material errors or misstatements that have occurred will not be detected by an IS auditor.

Overall audit risk - The probability that information or financial report may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under security so the overall audit risk is at sufficiently low level at the completion of the examination.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 50

http://en.wikipedia.org/wiki/Audit_risk

http://www.dummies.com/how-to/content/how-to-assess-inherent-risk-in-an-audit.html

Licensed to Berend Post berend.post@it-university.nl

http://pakaccountants.com/what-is-control-risk/

http://accounting-simplified.com/audit/risk-assessment/audit-risk.html

Question 2440

To gain a clear understanding of the impact that a new regulatory requirement will have on an organization's information security controls, an information security manager should FIRST:

- ☐ conduct a risk assessment.
- ☒ perform a gap analysis.
- ☐ conduct a cost-benefit analysis.
- ☐ interview senior management.

Question 2441

Which of the following BEST demonstrates effective information security management within an organization?

- ☐ Employees support decisions made by information security management.
- ☐ Excessive risk exposure in one department can be absorbed by other departments.
- ☒ Information security governance is incorporated into organizational governance.
- ☐ Control ownership is assigned to parties who can accept losses related to control failure.

Question 2442

An IS auditor observes that routine backups of operational databases are taking longer than before. Which of the following would MOST effectively help to reduce backup and recovery times for operational databases?

- ☐ Utilizing database technologies to achieve efficiencies
- ☐ Using solid storage device (SSD) media
- ☒ Requiring a combination of weekly full backups and daily differential backups
- ☐ Archiving historical data in accordance with the data retention policy

Licensed to Berend Post berend.post@it-university.nl

Question 2443

A recent audit identified duplicate software licenses and technologies. Which of the following would be MOST helpful to prevent this type of duplication in the future?

- ☐ Centralizing IT procurement and approval practices
- ☒ Updating IT procurement policies and procedures
- ☐ Conducting periodic inventory reviews
- ☐ Establishing a project management office

Question 2444

What is an effective control for granting temporary access to vendors and external support personnel?

- ☒ Creating user accounts that automatically expire by a predetermined date
- ☐ Creating permanent guest accounts for temporary use
- ☐ Creating user accounts that restrict logon access to certain hours of the day
- ☐ Creating a single shared vendor administrator account on the basis of least-privileged access

Explanation:

Explanation:

Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

Question 2445

Which of the following is the BEST reason for an organization to develop a business continuity plan?

- ☐ To develop a detailed description of information systems and processes
- ☐ To identify the users of information systems and processes
- ☒ To avoid the costs resulting from the failure of key systems and processes
- ☐ To establish business unit prioritization of systems, projects, and strategies

Explanation:

Reference: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Business-Continuity-Management-Audit-Assurance-Program.aspx

Licensed to Berend Post berend.post@it-university.nl

Question 2446

When should plans for testing for user acceptance be prepared?

- ☒ In the requirements definition phase of the systems-development project
- ☐ In the feasibility phase of the systems-development project
- ☐ In the design phase of the systems-development project
- ☐ In the development phase of the systems-development project

Explanation:

Explanation:

Plans for testing for user acceptance are usually prepared in the requirements definition phase of the systems-development project.

Question 2447

Which of the following is MOST important for an IS auditor to determine when reviewing how the organization's incident response team handles devices that may be involved in criminal activity?

- ☐ Whether devices are checked for malicious applications
- ☐ Whether the access logs are checked before seizing the devices
- ☐ Whether users have knowledge of their devices being examined
- ☒ Whether there is a chain of custody for the devices

Question 2448

The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?

- ☐ e-mails.
- ☒ MP3.
- ☐ MS Office.
- ☐ Word template.
- ☐ None of the choices.

Explanation:

Explanation:

"Most trojan horse programs are spread through e-mails. Some earlier trojan horse programs were bundled in "Root Kits". For example, the Linux Root Kit version 3 (lrk3) which was released in December 96 had tcp wrapper trojans included and enhanced in the kit. Portable devices that run Linux can also be affected by trojan horse. The Trojan.Linux.JBellz Trojan horse runs as a malformed .mp3 file."

Licensed to Berend Post berend.post@it-university.nl

Question 2449

The recovery point objective (RPO) is required in which of the following?

- ☐ Information security plan
- ☐ Incident response plan
- ☐ Disaster recovery plan
- ☒ Business continuity plan

Question 2450

Why would a database be renormalized?

- ☐ To ensure data integrity
- ☒ To increase processing efficiency
- ☐ To prevent duplication of data
- ☐ To save storage space

Explanation:

A database is renormalized when there is a need to improve processing efficiency.

There is, however, a risk to data integrity when this occurs. Since it implies the introduction of duplication, it will not likely allow saving of storage space.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 109).

Question 2451

Which of the following would be the MOST important information to include in a business case for an information security project in a highly regulated industry?

- ☐ Industry comparison analysis
- ☐ Critical audit findings
- ☒ Compliance risk assessment
- ☐ Number of reported security incidents

Licensed to Berend Post berend.post@it-university.nl

Question 2452

An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

- ☐ Consistency
- ☐ Isolation
- ☐ Durability
- ☒ Atomicity

Explanation:

Explanation:

Atomicity guarantees that either the entire transaction is processed or none of it is. Consistency ensures that the database is in a legal state when the transaction begins and ends, isolation means that, while in an intermediate state, the transaction data is invisible to external operations. Durability guarantees that a successful transaction will persist, and cannot be undone.

Question 2453

During the testing of the business continuity plan (BCP), which of the following methods of results analysis provides the BEST assurance that the plan is workable?

- ☐ Measurement of accuracy
- ☐ Elapsed time for completion of critical tasks
- ☒ Quantitatively measuring the results of the test
- ☐ Evaluation of the observed test results

Explanation:

It is important to have ways to measure the success of the plan and tests against the stated objectives. Therefore, results must be quantitatively gauged as opposed to an evaluation based only on observation. Quantitatively measuring the results of the test involves a generic statement measuring all the activities performed during BCP, which gives the best assurance of an effective plan. Although choices A and B are also quantitative, they relate to specific areas, or an analysis of results from one viewpoint, namely the accuracy of the results and the elapsed time.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 5: Disaster Recovery and Business Continuity (page 269).

Licensed to Berend Post berend.post@it-university.nl

Question 2454

Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

- ☐ System testing
- ☒ Acceptance testing
- ☐ Integration testing
- ☐ Unit testing

Explanation:

Explanation:

Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level, as this could result in delays and cost overruns. System testing is undertaken by the developer team to determine if the software meets user requirements per specifications. Integration testing examines the units/modules as one integrated system and unit testing examines the individual units or components of the software. System, integration and unit testing are all performed by the developers at various stages of development; the impact of failure is comparatively less for each than failure at the acceptance testing stage.

Question 2455

While evaluating logical access control the IS auditor should follow all of the steps mentioned below EXCEPT one?

1. Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc
2. Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
3. Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
4. Evaluate the access control environment to determine if the control objective is achieved by analyzing test result and other audit evidence
5. Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.
6. Evaluate and deploy technical controls to mitigate all identified risks during audit.

- ☐ 2
- ☐ 3
- ☐ 1
- ☒ 6

Explanation:

The word EXCEPT is the keyword used in the question. You need find out the item an IS auditor should not perform while evaluating logical access control. It is not an IT auditor's responsibility to evaluate and deploy technical controls to mitigate all identified risks during audit.

Licensed to Berend Post berend.post@it-university.nl

For CISA exam you should know below information about auditing logical access:

Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation,etc

Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness

Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique

Evaluate the access control environment to determine if the control objective are achieved by analyzing test result and other audit evidence

Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.

The following were incorrect answers:

The other options presented are valid choices which IS auditor needs to follow while evaluating logical access control.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 362

Question 2456

When planning an audit, it is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the:

- ☒ report was released within the last 12 months.
- ☐ scope and methodology meet audit requirements.
- ☐ service provider is independently certified and accredited.
- ☐ report confirms that service levels were not violated.

Licensed to Berend Post berend.post@it-university.nl

Question 2457

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

- ☐ Identify high-risk areas that might need a detailed review later
- ☐ Reduce audit costs
- ☒ Reduce audit time
- ☐ Increase audit accuracy

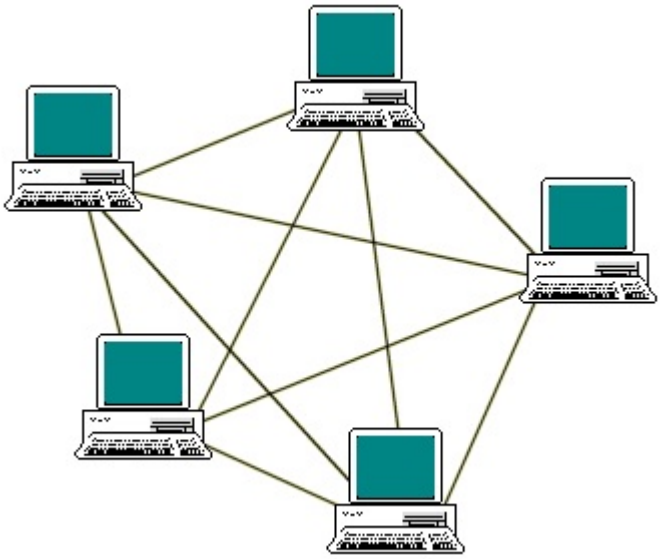
Explanation:

Explanation:

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

Question 2458

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☒ Mesh

Explanation:

For your exam you should know the information below related to LAN topologies:

LAN Topologies

Network topology is the physical arrangement of the various elements (links, nodes, etc.) of a computer network.

Licensed to Berend Post berend.post@it-university.nl

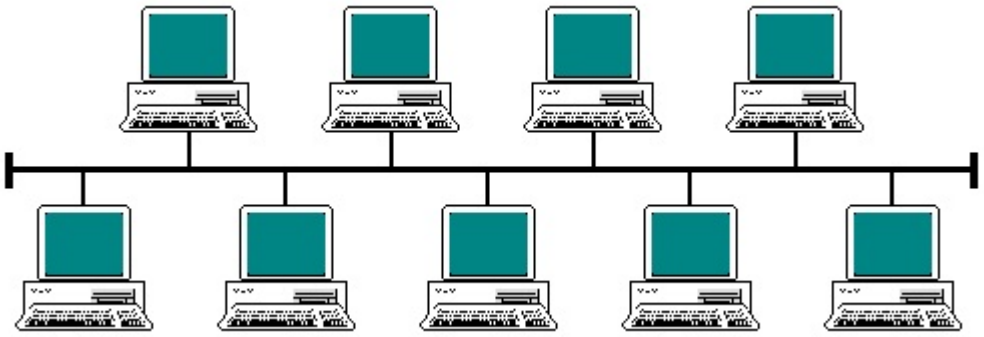
Essentially, it is the topological structure of a network, and may be depicted physically or logically. Physical topology refers to the placement of the network's various components, including device location and cable installation, while logical topology shows how data flows within a network, regardless of its physical design.

Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology



Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly

Licensed to Berend Post berend.post@it-university.nl

the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

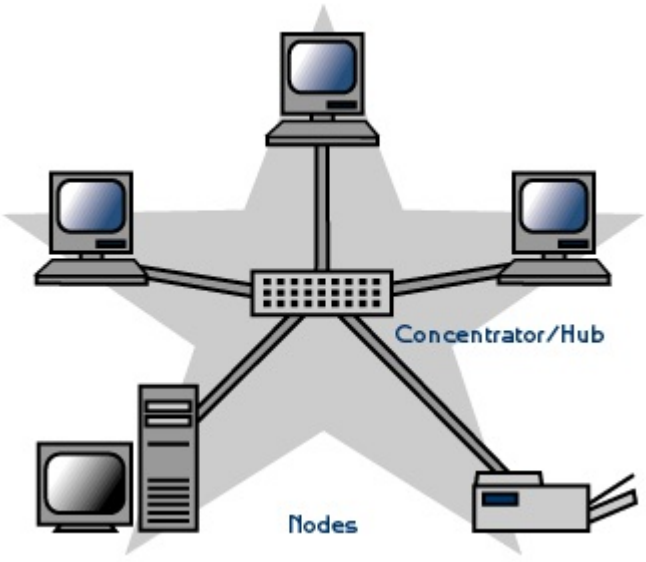
In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be connected to one central device.

All traffic that traverses the network passes through the central point. The central point acts as a signal repeater.

The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the central point represents a single point of failure.

Star Topology



Ring

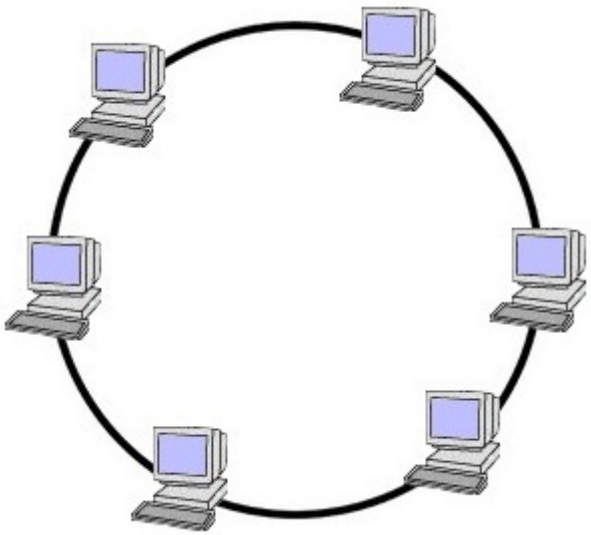
A network topology that is set up in a circular fashion in which data travels around the ring in one direction and each device on the ring acts as a repeater to keep the signal strong as it travels. Each

 Licensed to Berend Post berend.post@it-university.nl

device incorporates a receiver for the incoming signal and a transmitter to send the data on to the next device in the ring.

The network is dependent on the ability of the signal to travel around the ring. When a device sends data, it must travel through each device on the ring until it reaches its destination. Every node is a critical link. If one node goes down the whole link would be affected.

Ring Topology



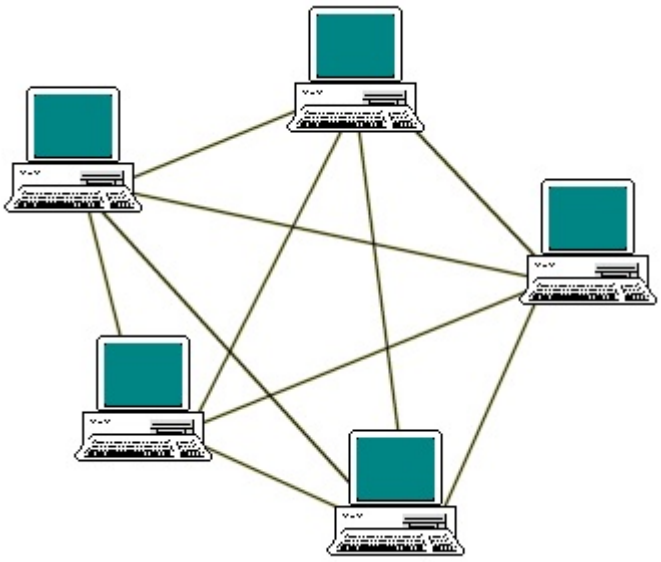
Mesh

The value of a fully meshed networks is proportional to the exponent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints, is approximated by Reed's Law.

A mesh network provides for high availability and redundancy. However, the cost of such network could be very expensive if dozens of devices are in the mesh.

Mesh Topology

Licensed to Berend Post berend.post@it-university.nl



Fully connected mesh topology

A fully connected network is a communication network in which each of the nodes is connected to each other. In graph theory it known as a complete graph. A fully connected network doesn't need to use switching nor broadcasting. However, its major disadvantage is that the number of connections grows quadratic ally with the number of nodes, so it is extremely impractical for large networks. A two-node network is technically a fully connected network.

Partially connected mesh topology

The type of network topology in which some of the nodes of the network are connected to more than one other node in the network with a point-to-point link – this makes it possible to take advantage of some of the redundancy that is provided by a physical fully connected mesh topology without the expense and complexity required for a connection between every node in the network.

The following answers are incorrect:

The other options presented are not valid.

The following reference(s) were/was used to create this question:

CISA review manual 2014, Page number 262

Licensed to Berend Post berend.post@it-university.nl

Question 2459

Which of the following is the MOST effective way to identify anomalous transactions when performing a payroll fraud audit?

- ☐ Substantive testing of payroll files
- ☒ Data analytics on payroll data
- ☐ Observation of payment processing
- ☐ Sample-based review of pay stubs

Question 2460

An IT steering committee assists the board of directors to fulfill IT governance duties by:

- ☐ developing IT policies and procedures for project tracking.
- ☐ focusing on the supply of IT services and products.
- ☒ overseeing major projects and IT resource allocation.
- ☐ implementing the IT strategy.

Question 2461

The implementation of access controls FIRST requires:

- ☐ a classification of IS resources.
- ☐ the labeling of IS resources.
- ☐ the creation of an access control list.
- ☒ an inventory of IS resources.

Question 2462

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

- ☐ Assigning copyright to the organization
- ☐ Program back doors
- ☒ Source code escrow
- ☐ Internal programming expertise

Explanation:

Explanation:

Source code escrow protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business.

Licensed to Berend Post berend.post@it-university.nl

Question 2463

Which of the following statement correctly describes the difference between QAT and UAT?

- ☒ QAT focuses on technical aspect of the application and UAT focuses on functional aspect of the application
- ☐ UAT focuses on technical aspect of the application and QAT focuses on functional aspect of the application
- ☐ UAT and QAT both focuses on functional aspect of the application
- ☐ UAT and QAT both focuses on technical aspect of the application

Explanation:

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.

For CISA exam you should know below types of testing:

Unit Testing – The testing of an individual program or module. Unit testing uses set of test cases that focus on control structure of procedural design. These tests ensure internal operation of the programs according to the specification.

Interface or integration testing – A hardware or software test that evaluates the connection of two or more components that pass information from one area to another. The objective it to take unit tested module and build an integrated structure dictated by design. The term integration testing is also referred to tests that verify and validate functioning of the application under test with other systems, where a set of data is transferred from one system to another.

System Testing – A series of tests designed to ensure that modified programs, objects, database schema, etc , which collectively constitute a new or modified system, function properly. These test procedures are often performed in a non-production test/development environment by software developers designated as a test team. The following specific analysis may be carried out during system testing.

Recovery Testing – Checking the system's ability to recover after a software or hardware failure.

Security Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems.

Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour.

Licensed to Berend Post berend.post@it-university.nl

Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process.

Stress Testing – Studying the impact on the application by testing with an incremental umber of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process.

Performance Testing – Comparing the system performance to other equivalent systems using well defined benchmarks.

Final Acceptance Testing -It has two major parts: Quality Assurance Testing(QAT) focusing on the technical aspect of the application and User acceptance testing focusing on functional aspect of the application.

QAT focuses on documented specifications and the technology employed. It verifies that application works as documented by testing the logical design and the technology itself. It also ensures that the application meet the documented technical specifications and deliverables. QAT is performed primarily by IS department. The participation of end user is minimal and on request. QAT does not focus on functionality testing.

UAT supports the process of ensuring that the system is production ready and satisfies all documented requirements. The methods include:

Definition of test strategies and procedure.

Design of test cases and scenarios

Execution of the tests.

Utilization of the result to verify system readiness.

Acceptance criteria are defined criteria that a deliverable must meet to satisfy the predefined needs of the user. A UAT plan must be documented for the final test of the completed system. The tests are written from a user's perspective and should test the system in a manner as close to production possible.

The following were incorrect answers:

The other presented options incorrectly describe the difference between QAT and UAT

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 166

Licensed to Berend Post berend.post@it-university.nl

Question 2464

Which of the following is the MOST effective way to prevent unauthorized changes from being moved into production?

- ☐ Conduct periodic review of change tickets to ensure all change documentation is attached.
- ☐ Enforce segregation of duties between developers and migrators.
- ☒ Perform thorough testing of changes in the test environment.
- ☐ Require approval of changes by the appropriate business process owners.

Question 2465

Which of the following message services provides the strongest evidence that a specific action has occurred?

- ☐ Proof of delivery
- ☒ Nonrepudiation
- ☐ Proof of submission
- ☐ Message origin authentication

Explanation:

Explanation:

Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts, i.e., proof of submission, proof of delivery and message origin authentication. However, nonrepudiation provides stronger evidence because the proof can be demonstrated to a third party. Digital signatures are used to provide nonrepudiation. Message origination authentication will only confirm the source of the message and does not confirm the specification that has been completed.

Question 2466

When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

- ☐ cost-benefit analysis
- ☒ regulatory requirements
- ☐ best practices
- ☐ control framework

Licensed to Berend Post berend.post@it-university.nl

Question 2467

An organization has a number of branches across a wide geographical area. To ensure that all aspects of the disaster recovery plan are evaluated in a cost effective manner, an IS auditor should recommend the use of a:

- ☐ data recovery test.
- ☐ full operational test.
- ☐ posttest.
- ☒ preparedness test.

Explanation:

Explanation:

A preparedness test should be performed by each local office/area to test the adequacy of the preparedness of local operations in the event of a disaster. This test should be performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence of the plan's adequacy. A data recovery test is a partial test and will not ensure that all aspects are evaluated. A full operational test is not the most cost effective test in light of the geographical dispersion of the branches, and a posttest is a phase of the test execution process.

Question 2468

As an outcome of information security governance, strategic alignment provides:

- ☒ security requirements driven by enterprise requirements.
- ☐ baseline security following best practices.
- ☐ institutionalized and commoditized solutions.
- ☐ an understanding of risk exposure.

Explanation:

Explanation:

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

Licensed to Berend Post berend.post@it-university.nl

Question 2469

An IS auditor reviews change control tickets and finds an emergency change request where an IT manager approved the change modified the code on the production platform, and resolved the ticket. Which of the following should be the auditor's GREATEST concern?

- ☐ There was no follow-up approval from the business.
- ☐ The change was made less than an hour after the request.
- ☐ There was no testing prior to making the change in production.
- ☒ The IT manager performed the change and resolved the ticket.

Question 2470

The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

- ☐ loss of confidentiality.
- ☒ increased redundancy.
- ☐ unauthorized accesses.
- ☐ application malfunctions.

Explanation:

Explanation:

Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional and otherwise unnecessary data handling efforts.

Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

Question 2471

An IS auditor reviewing the use of encryption finds that the symmetric key is sent by an email message between the parties. Which of the following audit responses is correct in this situation?

- ☐ An audit finding is recorded, as the key should be asymmetric and therefore changed.
- ☐ No audit finding is recorded, as it is normal to distribute a key of this nature in this manner.
- ☐ No audit finding is recorded, as the key can only be used once.
- ☒ An audit finding is recorded as the key should be distributed in a secure manner.

Licensed to Berend Post berend.post@it-university.nl

Question 2472

A CEO requests access to corporate documents from a mobile device that does not comply with organizational policy. The information security manager should FIRST:

- ☒ evaluate the business risk
- ☐ evaluate a third-party solution
- ☐ initiate an exception approval process
- ☐ deploy additional security controls

Question 2473

An IS auditor has discovered that unauthorized customer management software was installed on a workstation. The auditor determines the software has been uploading customer data to an external party. Which of the following is the IS auditor's BEST course of action?

- ☐ Review other workstations to determine the extent of the incident.
- ☐ Determine the number of customer records that were uploaded.
- ☒ Notify the incident response team.
- ☐ Present the issue at the next audit progress meeting.

Question 2474

Which of the following is the BEST guidance from an IS auditor to an organization planning an initiative to improve the effectiveness of its IT processes?

- ☐ IT staff should be surveyed to identify current IT process weaknesses and suggest improvements.
- ☒ The organization should use a capability maturity model to identify current maturity levels for each IT process.
- ☐ IT management should include process improvements in staff performance
- ☐ The organization should refer to prior audit reports to identify the specific IT processes to be improved.

Question 2475

What is an IS auditor's BEST recommendation to management if a review of the incident management process finds multiple instances of incident tickets remaining open for an unusually long time?

- ☐ Implement reporting of key performance indicators (KPIs) for ticket closure.
- ☐ Increase the number of help desk staff to enable faster ticket closure.
- ☐ Manually review the identified tickets and mark as closed in the system.
- ☒ Configure the system to automatically close tickets after a defined period.

Licensed to Berend Post berend.post@it-university.nl

Question 2476

Which of the following is the PRIMARY purpose of data classification?

- ☐ To determine access rights to data
- ☒ To provide a basis for protecting data
- ☐ To select encryption technologies
- ☐ To ensure integrity of data

Question 2477

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- ☐ Report the risks to the CIO and CEO immediately
- ☐ Examine e-business application in development
- ☒ Identify threats and likelihood of occurrence
- ☐ Check the budget available for risk management

Explanation:

Explanation: An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

Question 2478

Who is responsible for authorizing access level of a data user?

- ☒ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Explanation:

Data owners are responsible for authorizing access level of a data user. These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

For your exam you should know below roles in an organization

Data Owners – Data Owners are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access,

Licensed to Berend Post berend.post@it-university.nl

ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward –are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

Security Administrator -Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 361

Question 2479

Which of the following audit mainly focuses on discovering and disclosing on frauds and crimes?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☐ Integrated Audit
- ☒ Forensic audit

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice

For your exam you should know below information about different types of audit:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization's accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Licensed to Berend Post berend.post@it-university.nl

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

 Licensed to Berend Post berend.post@it-university.nl

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance Audit - A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Financial Audit- A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Integrated Audits - An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

Question 2480

An IS auditor is asked to identify risk within an organization's software development project. The project manager tells the auditor that an agile development methodology is being used to minimize the lengthy development process. Which of the following would be of GREATEST concern to the auditor?

- ☐ Each team does its own testing.
- ☒ The needed work has not yet been fully identified.
- ☐ Some of the developers have not attended recent training.
- ☐ Elements of the project have not been documented.

Question 2481

Which of the following PBX feature allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available?

- ☒ Automatic Call distribution
- ☐ Call forwarding
- ☐ Tenanting
- ☐ Voice mail

Explanation:

Automatic Call distribution allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

For your exam you should know below mentioned PBX features and Risks:

Licensed to Berend Post berend.post@it-university.nl

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Tapping and control of traffic

Call forwarding

Allow specifying an alternate number to which calls will be forwarded based on certain condition

User tracking

Account codes

Used to:

Track calls made by certain people or for certain projects for appropriate billing

Dial-In system access (user dials from outside and gain access to normal feature of the PBX)

Changing the user class of service so a user can access a different set of features (i.e. the override feature)

Fraud, user tracking, non authorized features

Access Codes

Key for access to specific feature from the part of users with simple instruments, i.e. traditional analog phones.

Non-authorized features

Silent Monitoring

Licensed to Berend Post berend.post@it-university.nl

Silently monitors other calls

Eavesdropping

Conferencing

Allows for conversation among several users

Eavesdropping, by adding unwanted/unknown parties to a conference

override(intrude)

Provides for the possibility to break into a busy line to inform another user an important message

Eavesdropping

Auto-answer

Allows an instrument to automatically go when called usually gives an auditor or visible warning which can easily turned off

Gaining information not normally available, for various purpose

Tenanting

Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Illegal usage, fraud, eavesdropping

Voice mail

Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Disclosure or destruction of all messages of a user when that user's password in known or discovered by an intruder, disabling of the voice mail system and even the entire switch by lengthy messages or embedded codes, illegal access to external lines.

Licensed to Berend Post berend.post@it-university.nl

Privacy release

Supports shared extensions among several devices, ensuring that only one device at a time can use an extension. Privacy release disables the security by allowing devices to connect to an extension already in use.

Eavesdropping

No busy extension

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Eavesdropping a conference in progress

Diagnostics

Allows for bypassing normal call restriction procedures. This kind of diagnostic is sometimes available from any connected device. It is a separate feature, in addition to the normal maintenance terminal or attendant diagnostics

Fraud and illegal usage

Camp-on or call waiting

When activated, sends a visual audible warning to an off-hook instrument that is receiving another call. Another option of this feature is to conference with the camped-on or call waiting

Making the called individual a party to a conference without knowing it.

Dedicated connections

Connections made through the PBX without using the normal dialing sequences. It can be used to create hot-lines between devices i.e. one rings when the other goes off-hook. It is also used for data connections between devices and the central processing facility

Eavesdropping on a line

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting - Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail - Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 358

Question 2482

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- ☐ create the procedures document.
- ☐ terminate the audit.
- ☐ conduct compliance testing.
- ☒ identify and evaluate existing practices.

Explanation:

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

Question 2483

The MOST effective control to detect fraud inside an organization's network, is to:

- ☐ implement an intrusion detection system (IDS)
- ☐ apply two-factor authentication
- ☒ review access logs
- ☐ segregate duties

Licensed to Berend Post berend.post@it-university.nl

Question 2484

Which of the following is an oft-cited cause of vulnerability of networks?

- ☒ software monoculture
- ☐ software diversification
- ☐ single line of defense
- ☐ multiple DMZ
- ☐ None of the choices.

Explanation:

Explanation:

An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.

Question 2485

An IS auditor finds that corporate mobile devices used by employees have varying levels of password settings. Which of the following would be the BEST recommendation?

- ☐ Update the acceptable use policy for mobile devices.
- ☐ Notify employees to set passwords to a specified length.
- ☐ Encrypt data between corporate gateway and devices.
- ☒ Apply a security policy to the mobile devices.

Question 2486

Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

- ☐ WAP is often configured by default settings and is thus insecure.
- ☐ WAP provides weak encryption for wireless traffic.
- ☒ WAP functions as a protocol-conversion gateway for wireless TLS to Internet SSL.
- ☐ WAP often interfaces critical IT systems.

Explanation:

Explanation:

Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL, the WAP gateway is a component warranting critical concern and review for the IS auditor when auditing and testing controls that enforce message confidentiality

Licensed to Berend Post berend.post@it-university.nl

Question 2487

Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

- ☐ key pair
- ☐ Oakley
- ☐ certificate
- ☐ 3-DES
- ☒ one-time pad
- ☐ None of the choices.

Explanation:

Explanation: It's possible to protect messages in transit by means of cryptography. One method of encryption - the one-time pad --has been proven to be unbreakable when correctly used. This method uses a matching pair of key- codes, securely distributed, which are used once-and-only-once to encode and decode a single message. Note that this method is difficult to use securely, and is highly inconvenient as well.

Question 2488

Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

- ☒ Redundancy check
- ☐ Completeness check
- ☐ Accuracy check
- ☐ Parity check

Explanation:

Explanation:

A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of data.

Question 2489

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

- ☐ has all the personnel and equipment it needs.
- ☒ plans are consistent with management strategy.
- ☐ uses its equipment and personnel efficiently and effectively.
- ☐ has sufficient excess capacity to respond to changing directions.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

Question 2490

IT service engineers at a large organization are unable to effectively prioritize system-generated alerts from hundreds of applications running across multiple servers and databases. As a result, many alerts are often ignored, leading to major problems including downtime. Which of the following is the BEST IS audit recommendation to address this situation?

- ☐ Prioritize alerts from legacy applications that may require remote support from external vendors.
- ☐ Implement a threshold management system that prioritizes alerts over a certain age.
- ☐ Develop a classification scheme that prioritizes alerts according to potential business impact.
- ☒ Group alerts from related systems and immediately escalate to the application owner.

Question 2491

Management has decided to include a compliance manager in the approval process for a new business that may require changes to the IT infrastructure. Which of the following is the GREATEST benefit of this approach?

- ☐ Security breach incidents can be identified in early stages.
- ☒ Regulatory risk exposures can be identified before they materialize.
- ☐ Fewer reviews are needed when updating the IT compliance process.
- ☐ Process accountabilities to external stakeholders are improved.

Question 2492

To ensure confidentiality through the use of asymmetric encryption, a message is encrypted with which of the following?

- ☐ Sender’s private key
- ☐ Recipient’s private key
- ☐ Sender’s public key
- ☒ Recipient’s public key

Licensed to Berend Post berend.post@it-university.nl

Question 2493

An IS auditor notes that a loan servicing group retains customer personally identifiable information (PII) on a shared drive. Which of the following is MOST important to ensure compliance with privacy principles?

- ☐ Backups are performed in accordance with organizational policy.
- ☐ Access to the shared drive must be approved by the manager of the group.
- ☒ The data is maintained in accordance with the business's retention policy.
- ☐ All key customer data elements are captured on the shared drive.

Question 2494

The most common problem in the operation of an intrusion detection system (IDS) is:

- ☒ the detection of false positives.
- ☐ receiving trap messages.
- ☐ reject-error rates.
- ☐ denial-of-service attacks.

Explanation:

Explanation:

Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents- false positives, the equivalent of a false alarm. An IS auditor needs to be aware of this and should check for implementation of related controls, such as IDS tuning, and incident handling procedures, such as the screening process to know if an event is a security incident or a false positive. Trap messages are generated by the Simple Network Management Protocol (SNMP) agents when an important event happens, but are not particularly related to security or IDSs.

Reject-error rate is related to biometric technology and is not related to IDSs. Denial-of-service is a type of attack and is not a problem in the operation of IDSs.

Question 2495

Which of the following is the BEST approach for performing a business impact analysis (BIA) of a supply-chain management application?

- ☐ Circulating questionnaires to key internal stakeholders
- ☐ Interviewing groups of key stakeholders
- ☐ Accepting IT personnel's view of business issues
- ☒ Reviewing the organization's policies and procedures

Licensed to Berend Post berend.post@it-university.nl

Question 2496

What is the BEST indicator of successful implementation of an organization's information security policy?

- ☐ Reduced number of successful phishing incidents
- ☐ Reduced number of help desk calls
- ☒ Reduced number of noncompliance penalties incurred
- ☐ Reduced number of false-positive security events

Question 2497

Which of the following is an example of a change to the external threat landscape?

- ☐ Organizational security standards have been modified.
- ☒ A commonly used encryption algorithm has been compromised.
- ☐ New legislation has been enacted in a region where the organization does business.
- ☐ Infrastructure changes to the organization have been implemented.

Question 2498

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- ☐ central processing site after running the application system.
- ☐ central processing sire during the running of the application system.
- ☐ remote processing site after transmission of the data to the central processing site.
- ☒ remote processing site prior to transmission of the data to the central processing site.

Explanation:

Explanation:

It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

Question 2499

Which of the following is best suited for searching for address field duplications?

- ☐ Text search forensic utility software
- ☒ Generalized audit software
- ☐ Productivity audit software
- ☐ Manual review

Explanation:

Explanation:

Generalized audit software can be used to search for address field duplications.

Licensed to Berend Post berend.post@it-university.nl

Question 2500

Which of the following projects would be MOST important to review in an audit of an organization's financial statements?

- ☐ Resource optimization of the enterprise resource planning (ERP) system
- ☐ Security enhancements to the customer relationship database
- ☐ Automation of operational risk management processes
- ☒ Outsourcing of the payroll system to an external service provider

Question 2501

Which of the following is an advantage of asymmetric crypto system over symmetric key crypto system?

- ☐ Performance and Speed
- ☒ Key Management is built in
- ☐ Adequate for Bulk encryption
- ☐ Number of keys grows very quickly

Explanation:

Key management is better in asymmetric key encryption as compare to symmetric key encryption. In fact, there is no key management built within Symmetric Crypto systems. You must use the sneaker net or a trusted courier to exchange the key securely with the person you wish to communicate with.

Key management is the major issue and challenge in symmetric key encryption.

In symmetric key encryption, a symmetric key is shared between two users who wish to communicate together. As the number of users grows, the number of keys required also increases very rapidly.

For example, if a user wants to communicate with 5 different users then total number of different keys required by the user are 10. The formula for calculating total number of key required is n(n-1)/2Or total number of users times total of users minus one divided by 2.

Where n is number of users communicating with each others securely.

In an asymmetric key encryption, every user will have only two keys, also referred to as a Key Pair.

Private Key – Only known to the user who initially generated the key pair

Public key – Known to everyone, can be distributed at large

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Performance – Symmetric key encryption performance is better than asymmetric key encryption

Bulk encryption – As symmetric key encryption gives better performance, symmetric key should be used for bulk data encryption

Number of keys grows very quickly - The number of keys under asymmetric grows very nicely.1000 users would need a total of only 2000 keys, or a private and a public key for each user. Under symmetric encryption, one thousand users would need 495,000 keys to communicate securely with each others.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

Question 2502

Which of the following should an IS auditor recommend to reduce the likelihood of potential intruders using social engineering?

- ☐ Perform simulated attacks.
- ☐ Prohibit the use of social networking platforms.
- ☐ Implement an intrusion detection system (IDS).
- ☒ Deploy a security awareness program.

Question 2503

The use of risk assessment tools for classifying risk factors should be formalized in your IT audit effort through:

- ☐ the use of risk controls.
- ☐ the use of computer assisted functions.
- ☐ using computer assisted audit technology tools.
- ☒ the development of written guidelines.
- ☐ None of the choices.

Explanation:

Explanation:

A successful risk-based IT audit program could be based on an effective scoring system. In establishing a scoring system, management should consider all relevant risk factors and avoid subjectivity. Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee.

Licensed to Berend Post berend.post@it-university.nl

Question 2504

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

- ☐ include the statement of management in the audit report.
- ☒ identify whether such software is, indeed, being used by the organization.
- ☐ reconfirm with management the usage of the software.
- ☐ discuss the issue with senior management since reporting this could have a negative impact on the organization.

Explanation:

Explanation:

When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

Question 2505

Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

- ☐ Acceptance testing is to be managed by users.
- ☒ A quality plan is not part of the contracted deliverables.
- ☐ Not all business functions will be available on initial implementation.
- ☐ Prototyping is being used to confirm that the system meets business requirements.

Explanation:

Explanation:

A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 2506

Which is MOST important when contracting an external party to perform a penetration test?

- ☐ Obtain approval from IT management.
- ☒ Define the project scope.
- ☐ Increase the frequency of log reviews.
- ☐ Provide network documentation.

Question 2507

Which of the following would effectively verify the originator of a transaction?

- ☐ Using a secret password between the originator and the receiver
- ☐ Encrypting the transaction with the receiver's public key
- ☐ Using a portable document format (PDF) to encapsulate transaction content
- ☒ Digitally signing the transaction with the source's private key

Explanation:

Explanation:

A digital signature is an electronic identification of a person, created by using a public key algorithm, to verify to a recipient the identity of the source of a transaction and the integrity of its content. Since they are a 'shared secret' between the user and the system itself, passwords are considered a weaker means of authentication. Encrypting the transaction with the recipient's public key will provide confidentiality for the information, while using a portable document format(PDF) will probe the integrity of the content but not necessarily authorship.

Question 2508

Which of the following would be the BEST way to address segregation of duties issues in an organization with budget constraints?

- ☐ Perform an independent audit.
- ☐ Rotate job duties periodically.
- ☒ Implement compensating controls.
- ☐ Hire temporary staff.

Licensed to Berend Post berend.post@it-university.nl

Question 2509

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- ☐ A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- ☐ Firewall policies are updated on the basis of changing requirements.
- ☐ inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- ☒ The firewall is placed on top of the commercial operating system with all installation options.

Explanation:

Explanation:

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

Question 2510

What is an initial step in creating a proper firewall policy?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Determining appropriate firewall hardware and software
- ☒ Identifying network applications such as mail, web, or FTP servers
- ☐ Configuring firewall access rules

Explanation:

Explanation:

Identifying network applications such as mail, web, or FTP servers to be externally accessed is an initial step in creating a proper firewall policy.

Licensed to Berend Post berend.post@it-university.nl

Question 2511

When segregation of duties concerns exists between IT support staff and end users, what would be suitable compensating control?

- ☐ Restricting physical access to computing equipment
- ☒ Reviewing transaction and application logs
- ☐ Performing background checks prior to hiring IT staff
- ☐ Locking user sessions after a specified period of inactivity

Explanation:

Explanation:

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

Question 2512

Attack amplifier is often being HEAVILY relied upon on by which of the following types of attack?

- ☐ Packet dropping
- ☐ ToS
- ☒ DDoS
- ☐ ATP
- ☐ Wiretapping
- ☐ None of the choices.

Explanation:

Explanation:

Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts are used to flood a target system with network requests. One technique to exhaust victim resources is through the use of an attack amplifier - where the attacker takes advantage of poorly designed protocols on 3rd party machines in order to instruct these hosts to launch the flood.

Licensed to Berend Post berend.post@it-university.nl

Question 2513

To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

- ☐ access control servers.
- ☒ session border controllers.
- ☐ backbone gateways.
- ☐ intrusion detection system (IDS).

Explanation:

Explanation:

Session border controllers enhance the security in the access network and in the core. In the access network, they hide a user's real address and provide a managed public address. This public address can be monitored, minimizing the opportunities for scanning and denial-of-service (DoS) attacks. Session border controllers permit access to clients behind firewalls while maintaining the firewall's effectiveness. In the core, session border controllers protect the users and the network. They hide network topology and users' real addresses. They can also monitor bandwidth and quality of service. Securing the access control server, backbone gateways and intrusion detection systems (IDSs) does not effectively protect against DoS attacks.

Question 2514

An organization has made a strategic decision to split into separate operating entities to improve profitability. However, the IT infrastructure remains shared between the entities. Which of the following would BEST help to ensure that IS audit still covers key risk areas within the IT environment as part of its annual plan?

- ☐ Increasing the frequency of risk-based IS audits for each business entity
- ☐ Revising IS audit plans to focus on IT changes introduced after the split
- ☐ Conducting an audit of newly introduced IT policies and procedures
- ☒ Developing a risk-based plan considering each entity's business processes

Question 2515

IT best practices for the availability and continuity of IT services should:

- ☐ minimize costs associated with disaster-resilient components.
- ☐ provide for sufficient capacity to meet the agreed upon demands of the business.
- ☒ provide reasonable assurance that agreed upon obligations to customers can be met.
- ☐ produce timely performance metric reports.

Explanation:

Explanation:

It is important that negotiated and agreed commitments (i.e., service level agreements [SLAs]) can be fulfilled all the time. If this were not achievable, IT should not have agreed to these requirements, as entering into such a commitment would be misleading to the business. 'All the time' in this context

Licensed to Berend Post berend.post@it-university.nl

directly relates to the 'agreed obligations' and does not imply that a service has to be available 100 percent of the time. Costs are a result of availability and service continuity management and may only be partially controllable. These costs directly reflect the agreed upon obligations. Capacity management is a necessary, but not sufficient, condition of availability.

Despite the possibility that a lack of capacity may result in an availability issue, providing the capacity necessary for seamless operations of services would be done within capacity management, and not within availability management. Generating reports might be a task of availability and service continuity management, but that is true for many other areas of interest as well (e.g., incident, problem, capacity and change management).

Question 2516

Which of the following would contribute MOST to an effective business continuity plan (BCP)?

- ☐ Document is circulated to all interested parties
- ☒ Planning involves all user departments
- ☐ Approval by senior management
- ☐ Audit by an external IS auditor

Explanation:

Explanation:

The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users. Though essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

Question 2517

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

- ☐ Overlapping controls
- ☐ Boundary controls
- ☐ Access controls
- ☒ Compensating controls

Explanation:

Explanation:

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated.

Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-

Licensed to Berend Post berend.post@it-university.nl

be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

Question 2518

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- ☐ analysis.
- ☐ evaluation.
- ☒ preservation.
- ☐ disclosure.

Explanation:

Explanation:

Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important but not of primary concern in a forensic investigation.

Question 2519

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do?

- ☐ Lack of IT documentation is not usually material to the controls tested in an IT audit.
- ☐ The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.
- ☒ The auditor should at least document the informal standards and policies, and test for a compliance. Furthermore, the IS auditor should recommend management that formal documented policies be developed and implemented.
- ☐ The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

Explanation:

Explanation:

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

Licensed to Berend Post berend.post@it-university.nl

Question 2520

Which of the following hardware upgrades would BEST enhance the capability of a web server to accommodate a significant increase in web traffic?

- ☒ Multicore CPUs
- ☐ Solid state drives
- ☐ Additional flash memory
- ☐ Cloud architecture

Question 2521

John is the product manager for an information system. His product has undergone under security review by an IS auditor. John has decided to apply appropriate security controls to reduce the security risks suggested by an IS auditor. Which of the following technique is used by John to treat the identified risk provided by an IS auditor?

- ☒ Risk Mitigation
- ☐ Risk Acceptance
- ☐ Risk Avoidance
- ☐ Risk transfer

Explanation:

Explanation:

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented.

For your exam you should know below information about risk assessment and treatment:

A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. A risk assessment is carried out, and the results are analyzed. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much security, not enough security, or the wrong security controls, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of resources that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

Identify assets and their value to the organization.

Identify vulnerabilities and threats.

Quantify the probability and business impact of these potential threats.

Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Licensed to Berend Post berend.post@it-university.nl

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance.

It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before committing to owning, insuring, and driving a motor vehicle.

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if, indeed, the company

Licensed to Berend Post berend.post@it-university.nl

has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could have a catastrophic effect on the company's ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase of new hardware, software, and office equipment, while transference of the risk to an insurance company would require premium payments. The

executive then further notes that minimal impact to the organization would occur if any of the reported low-level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to forgo the costs and accept the risk. In the young driver example, risk acceptance could be based on the observation that the youngster has demonstrated the responsibility and maturity to warrant the parent's trust in his or her judgment.

The following answers are incorrect:

Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

Risk Avoidance - Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized.

Risk Acceptance - Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA Review Manual 2014 Page number 51

Official ISC2 guide to CISSP CBK 3rd edition page number 383,384 and 385

Question 2522

A decision support system (DSS):

- ☐ is aimed at solving highly structured problems.
- ☐ combines the use of models with nontraditional data access and retrieval functions.
- ☒ emphasizes flexibility in the decision making approach of users.
- ☐ supports only structured decision making tasks.

Explanation:

Explanation:

DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semi structured decision making tasks.

Question 2523

A large number of exceptions to an organization's information security standards have been granted after senior management approved a bring your own device (BYOD) program. To address this situation, it is MOSTimportant for the information security manage to:

- ☐ introduce strong authentication on devices
- ☐ reject new exception requests
- ☐ require authorization to wipe lost devices
- ☒ update the information security policy

Question 2524

IS audits should be selected through a risk analysis process to concentrate on:

- ☒ those areas of greatest risk and opportunity for improvements.
- ☐ those areas of least risk and opportunity for improvements.
- ☐ those areas of the greatest financial value.
- ☐ areas led by the key people of the organization.
- ☐ random events.
- ☐ irregular events.

Explanation:

Explanation:

Audits are typically selected through a risk analysis process to concentrate on those areas of greatest risk and opportunity for improvements.

Licensed to Berend Post berend.post@it-university.nl

Audit topics are supposed to be chosen based on potential for cost savings and service improvements.

Question 2525

During a database audit, an IS auditor noted frequent problems due to the growing size of the order tables. Which of the following is the BEST recommendation in this situation?

- ☒ Develop an archiving approach.
- ☐ Periodically delete completed orders.
- ☐ Build more table indices.
- ☐ Migrate to a different database management system.

Question 2526

Ideally, stress testing should be carried out in a:

- ☐ test environment using test data.
- ☐ production environment using live workloads.
- ☒ test environment using live workloads.
- ☐ production environment using test data.

Explanation:

Explanation:

Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices Band D), and if only test data is used, there is no certainty that the system was stress tested adequately.

Question 2527

Which of the following statements regarding an off-site information processing facility is TRUE?

- ☒ It should have the same amount of physical access restrictions as the primary processing site.
- ☐ It should be located in proximity to the originating site so that it can quickly be made operational.
- ☐ It should be easily identified from the outside so in the event of an emergency it can be easily found.
- ☐ Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive.

Explanation:

It is very important that the offsite has the same restrictions in order to avoided misuse.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect because:

It should be located in proximity to the originating site so that it can quickly be made operational is incorrect as the offsite is also subject to the same disaster as of the primary site.

It should be easily identified from the outside so in the event of an emergency it can be easily found is also incorrect as it should not be easily identified to prevent intentional sabotage.

Need not have the same level of environmental monitoring as the originating site since this would be cost prohibitive is also incorrect as it should be like its primary site.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 265).

Question 2528

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

- ☐ EDI trading partner agreements.
- ☐ physical controls for terminals.
- ☒ authentication techniques for sending and receiving messages.
- ☐ program change control procedures.

Explanation:

Explanation:

Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

Question 2529

Which of the following is the BEST physical security solution for granting and restricting access to individuals based on their unique access needs?

- ☐ Bolting door locks
- ☐ Cipher locks
- ☐ Closed-circuit television (CCTV)
- ☒ Electronic badge system

Licensed to Berend Post berend.post@it-university.nl

Question 2530

The technique used to ensure security in virtual private networks (VPNs) is:

- ☒ encapsulation.
- ☐ wrapping.
- ☐ transform.
- ☐ encryption

Explanation:

Explanation: Encapsulation, or tunneling, is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly. The original packet is wrapped in another packet. The other choices are not security techniques specific to VPNs.

Question 2531

In determining the acceptable time period for the resumption of critical business processes:

- ☐ only downtime costs need to be considered.
- ☐ recovery operations should be analyzed.
- ☒ both downtime costs and recovery costs need to be evaluated.
- ☐ indirect downtime costs should be ignored.

Explanation:

Explanation:

Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to recover information resources might be prohibitive for nonessential business processes. Recovery operations do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows incurred due to business disruption. The indirect costs of a serious disruption to normal business activity, e.g., loss of customer and supplier goodwill and loss of market share, may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

Licensed to Berend Post berend.post@it-university.nl

Question 2532

An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

- ☐ The tools used to conduct the test
- ☐ Certifications held by the IS auditor
- ☒ Permission from the data owner of the server
- ☐ An intrusion detection system (IDS) is enabled

Explanation:

Explanation:

The data owner should be informed of the risks associated with a penetration test, what types of tests are to be conducted and other relevant details. All other choices are not as important as the data owner's responsibility for the security of the data assets.

Question 2533

Which of the following could provide an organization with the fastest resumption of processing following a disk failure?

- ☐ Server load balancing
- ☒ Mirroring
- ☐ Open database connectivity (ODBC) of the backup server
- ☐ Replication

Question 2534

To support an organization's goals, an IS department should have:

- ☐ a low-cost philosophy.
- ☒ long- and short-range plans.
- ☐ leading-edge technology.
- ☐ plans to acquire new hardware and software.

Explanation:

Explanation:

To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

Licensed to Berend Post berend.post@it-university.nl

Question 2535

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

- ☐ record the observations separately with the impact of each of them marked against each respective finding.
- ☐ advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
- ☒ record the observations and the risk arising from the collective weaknesses.
- ☐ apprise the departmental heads concerned with each observation and properly document it in the report.

Explanation:

Explanation:

Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined effect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

Question 2536

Which of the following append themselves to files as a protection against viruses?

- ☐ Behavior blockers
- ☐ Cyclical redundancy checkers (CRCs)
- ☒ Immunizers
- ☐ Active monitors

Explanation:

Explanation:

Immunizers defend against viruses by appending sections of themselves to files. They continuously check the file for changes and report changes as possible viral behavior. Behavior blockers focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record, or making changes to executable files. Cyclical redundancy checkers compute a binary number on a known virus-free program that is then stored in a database file. When that program is subsequently called to be executed, the checkers look for changes to the files, compare it to the database and report possible infection if changes have occurred. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions.

Licensed to Berend Post berend.post@it-university.nl

Question 2537

When implementing an application software package, which of the following presents the GREATEST risk?

- ☐ Uncontrolled multiple software versions
- ☐ Source programs that are not synchronized with object code
- ☒ incorrectly set parameters
- ☐ Programming errors.

Explanation:

Explanation:

Parameters that are not set correctly would be the greatest concern when implementing an application software package. The other choices, though important, are a concern of the provider, not the organization that is implementing the software itself.

Question 2538

Which of the following is the MOST important activity to undertake to avoid rework later in a project?

- ☐ Control review
- ☐ Risk assessment
- ☐ Acceptance testing
- ☒ Phase review

Question 2539

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- ☒ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Explanation:

PERMANENTLY is the keyword used in the question. You need to find out data removal method which remove data permanently from magnetic media.

Degaussing is the most effective method out of all provided choices to erase sensitive data on magnetic media provided magnetic media is not requiring to be reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

Licensed to Berend Post berend.post@it-university.nl

A device that performs degaussing generates a coercive magnetic force that reduces the magnetic flux density of the storage media to zero. This magnetic force is what properly erases data from media. Data are stored on magnetic media by the representation of the polarization of the atoms. Degaussing changes this polarization (magnetic alignment) by using a type of large magnet to bring it back to its original flux (magnetic alignment).

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed.

Simply deleting files or formatting the media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides.

Specialized hardware devices known as degausses can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist.

Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There is a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten.

To provide higher assurance in this case, it is necessary to overwrite each sector multiple times. Security practitioners should keep in mind that a one-time pass may be acceptable for noncritical information, but sensitive data should be overwritten with multiple passes. Overwrite software can also be used to clear the sectors within solid-state media such as USB thumb drives. It is suggested

 Licensed to Berend Post berend.post@it-university.nl

that physical destruction methods such as incineration or secure recycling should be considered for solid-state media that is no longer used.

The last form of preventing unauthorized access to sensitive data is media destruction. Shredding, burning, grinding, and pulverizing are common methods of physically destroying media. Degaussing can also be a form of media destruction. High-power degausses are so strong in some cases that they can literally bend and warp the platters in a hard drive.

Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine.

However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal.

The following answers are incorrect:

Overwrite every sector of magnetic media with pattern of 1's and 0's-Less effective than degaussing provided magnetic media is not requiring to be reuse.

Format magnetic media – Formatting magnetic media does not erase all data. Data can be recoverable after formatting using software tools.

Delete File allocation table-It will not erase all data. Data can be recoverable using software tools.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 338

Official ISC2 guide to CISSP CBK 3rd Edition Page number 720.

Licensed to Berend Post berend.post@it-university.nl

Question 2540

Which of the following should an IS auditor determine FIRST when evaluating additional hardware required to support the acquisition of a new accounting system?

- ☐ A training program has been developed to support the new accounting system.
- ☐ The supplier has experience supporting accounting systems.
- ☒ The hardware specified will be compliant with the current IT strategy.
- ☐ The hardware will be installed in a secure and environmentally controlled area.

Question 2541

Which of the following term related to network performance refers to the maximum rate that information can be transferred over a network?

- ☒ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Explanation:

In computer networks, bandwidth is often used as a synonym for data transfer rate - it is the amount of data that can be carried from one point to another in a given time period (usually a second).

This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A modem that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps. In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation.

It should be remembered that a real communications path usually consists of a succession of links, each with its own bandwidth. If one of these is much slower than the rest, it is said to be a bandwidth bottleneck.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Licensed to Berend Post berend.post@it-university.nl

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 page number 275

Question 2542

Which of the following is MOST likely to result from a business process reengineering (BPR) Project?

- ☒ An increased number of people using technology
- ☐ Significant cost saving, through a reduction the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Explanation:

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:

B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.

D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

Question 2543

Which of the following is a detective control?

- ☐ Procedures for authorizing transactions
- ☒ Echo checks in telecommunications
- ☐ A router rule restricting a service
- ☐ Programmed edit checks

Question 2544

What is the BEST action to prevent loss of data integrity or confidentiality in the case of an e-commerce application running on a LAN, processing electronic fund transfers (EFT) and orders?

- ☒ Using virtual private network (VPN) tunnels for data transfer
- ☐ Enabling data encryption within the application
- ☐ Auditing the access control to the network
- ☐ Logging all changes to access lists

Explanation:

Explanation:

The best way to ensure confidentiality and integrity of data is to encrypt it using virtual private network (VPN) tunnels. This is the most common and convenient way to encrypt the data traveling over the network. Data encryption within the application is less efficient than VPN. The other options

Licensed to Berend Post berend.post@it-university.nl

are good practices, but they do not directly prevent the loss of data Integrity and confidentiality during communication through a network.

Question 2545

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

- ☐ Overwriting the tapes
- ☐ initializing the tape labels
- ☒ Degaussing the tapes
- ☐ Erasing the tapes

Explanation:

Explanation:

The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely.

Initializing the tape labels would not remove the data that follows the label.

Question 2546

The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

- ☒ only the sender and receiver are able to encrypt/decrypt the data.
- ☐ the sender and receiver can authenticate their respective identities.
- ☐ the alteration of transmitted data can be detected.
- ☐ the ability to identify the sender by generating a one-time session key.

Explanation:

Explanation:

SSL generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality. Although SSL allows the exchange of X509 certificates to provide for identification and authentication, this feature along with choices C and D are not the primary objectives.

Question 2547

The reason a certification and accreditation process is performed on critical systems is to ensure that:

- ☒ security compliance has been technically evaluated.
- ☐ data have been encrypted and are ready to be stored.
- ☐ the systems have been tested to run on different platforms.
- ☐ the systems have followed the phases of a waterfall model.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

Question 2548

Which of the following is the GREATEST risk associated with the lack of an effective data privacy program?

- ☐ Failure to prevent fraudulent transactions
- ☐ Inability to manage access to private or sensitive data
- ☐ Inability to obtain customer confidence
- ☒ Failure to comply with data-related regulations

Question 2549

When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

- ☐ an integrated services digital network (ISDN) data link.
- ☒ traffic engineering.
- ☐ wired equivalent privacy (WEP) encryption of data.
- ☐ analog phone terminals.

Explanation:

Explanation:

To ensure that quality of service requirements are achieved, the Voice-over IP (VoIP) service over the wide area network (WAN) should be protected from packet losses, latency or jitter. To reach this objective, the network performance can be managed using statistical techniques such as traffic engineering. The standard bandwidth of an integrated services digital network (ISDN) data link would not provide the quality of services required for corporate VoIP services. WEP is an encryption scheme related to wireless networking. The VoIP phones are usually connected to a corporate local area network (LAN) and are not analog.

Licensed to Berend Post berend.post@it-university.nl

Question 2550

Which of the following is the MOST significant risk an IS auditor should consider when reviewing a credit card company's application system?

- ☒ Data privacy
- ☐ Processing times
- ☐ System availability
- ☐ Credit ratings

Question 2551

Which of the following is the PRIMARY benefit of implementing configuration management for IT?

- ☐ It helps audit in verifying IT conformance to business requirements.
- ☐ It establishes the dependency of application systems with various IT assets.
- ☐ It provides visibility to the overall function and technical attributes of IT assets.
- ☒ It helps automate change and release management processes in IT.

Question 2552

The risk that the IS auditor will not find an error that has occurred is identified by which of the following terms?

- ☐ Control
- ☐ Prevention
- ☐ Inherent
- ☒ Detection

Question 2553

Which of the following security control is intended to bring environment back to regular operation?

- ☐ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☒ Recovery

Explanation:

Explanation:

Recovery controls are intended to bring the environment back to regular operations

For your exam you should know below information about different security controls

Licensed to Berend Post berend.post@it-university.nl

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology

 Licensed to Berend Post berend.post@it-university.nl

or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to

 Licensed to Berend Post berend.post@it-university.nl

stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring

Corrective - Corrective control fixes components or systems after an incident has occurred

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Licensed to Berend Post berend.post@it-university.nl

Question 2554

Which of the following layer from an enterprise data flow architecture captures all data of interest to an organization and organize it to assist in reporting and analysis?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☒ Core data warehouse
- ☐ Data access layer

Explanation:

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Licensed to Berend Post berend.post@it-university.nl

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and

 Licensed to Berend Post berend.post@it-university.nl

context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Licensed to Berend Post berend.post@it-university.nl

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 2555

Which of the following is the MOST important incident management consideration for an organization subscribing to a cloud service?

- ☐ Decision on the classification of cloud-hosted data
- ☐ Expertise of personnel providing incident response
- ☐ Implementation of a SIEM in the organization
- ☒ An agreement on the definition of a security incident

Question 2556

Which of the following is MOST important for an IS auditor to verify after finding repeated unauthorized access attempts were recorded on a security report?

- ☐ Password reset requests have been confirmed as legitimate
- ☒ There is evidence that the incident was investigated
- ☐ System configuration changes are properly tracked
- ☐ A comprehensive access policy has been established

Question 2557

An organization is implementing the use of mobile devices that will connect to sensitive corporate applications. Which of the following is the BEST recommendation to mitigate risk of data leakage?

- ☐ Remote data wipe
- ☐ GPS tracking software
- ☐ Encrypted RFID tags
- ☒ Data encryption

Licensed to Berend Post berend.post@it-university.nl

Question 2558

Neural networks are effective in detecting fraud because they can:

- ☐ discover new trends since they are inherently linear.
- ☐ solve problems where large and general sets of training data are not obtainable.
- ☒ attack problems that require consideration of a large number of input variables.
- ☐ make assumptions about the shape of any curve relating variables to the output.

Explanation:

Explanation:

Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

Question 2559

The PRIMARY reason an IS department should analyze past incidents and problems is to:

- ☐ determine if all incidents and problems are reported.
- ☐ assign responsibility for problems.
- ☐ assess help desk performance.
- ☒ identify the causes of recurring incidents and problems.

Question 2560

Which of the following would be considered the BEST compensating control to use when an emergency process, rather than the established control procedures, is used for database changes?

- ☐ Using an emergency user account with the access to make changes to the database
- ☐ Using the administrator's own account to make out-of-hours changes
- ☒ Logging detailed before-and-after images for later review by the administrator
- ☐ Logging user's ID and change details for later review by the administrator

Licensed to Berend Post berend.post@it-university.nl

Question 2561

Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure with digital certificates for its business-to-consumer transactions via the internet?

- ☐ Customers are widely dispersed geographically, but the certificate authorities are not.
- ☐ Customers can make their transactions from any computer or mobile device.
- ☐ The certificate authority has several data processing subcenters to administer certificates.
- ☒ The organization is the owner of the certificate authority.

Explanation:

Explanation: If the certificate authority belongs to the same organization, this would generate a conflict of interest. That is, if a customer wanted to repudiate a transaction, they could allege that because of the shared interests, an unlawful agreement exists between the parties generating the certificates, if a customer wanted to repudiate a transaction, they could argue that there exists a bribery between the parties to generate the certificates, as shared interests exist. The other options are not weaknesses.

Question 2562

Which of the following is a good time frame for making changes to passwords?

- ☐ every 180 to 365 days
- ☐ every 30 to 45 days
- ☐ every 10 to 20 days
- ☒ every 90 to 120 days
- ☐ None of the choices.

Explanation:

Explanation:

"Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters. You may want to run a "password cracker" program periodically, and require users to immediately change any easily cracked passwords. In any case ask them to change their passwords every 90 to 120 days."

Licensed to Berend Post berend.post@it-university.nl

Question 2563

The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

- ☒ connecting points are available in the facility to connect laptops to the network.
- ☐ users take precautions to keep their passwords confidential.
- ☐ terminals with password protection are located in insecure locations.
- ☐ terminals are located within the facility in small clusters under the supervision of an administrator.

Explanation:

Explanation: Any person with wrongful intentions can connect a laptop to the network. The insecure connecting points, make unauthorized access possible if the individual has knowledge of a valid user ID and password. The other choices are controls for preventing unauthorized network access. If system passwords are not readily available for intruders to use, they must guess, introducing an additional factor and requires time. System passwords provide protection against unauthorized use of terminals located in insecure locations. Supervision is a very effective control when used to monitor access to a small operating unit or production resources.

Question 2564

Which of the following would MOST effectively aid executive management in achieving IT and business alignment?

- ☐ Risk assessment
- ☐ Value delivery assessment
- ☒ Balanced scorecard
- ☐ Performance measurement

Question 2565

Which of the following BEST enables effective closure of noncompliance issues?

- ☐ Insuring against the risk
- ☐ Performing control self-assessments
- ☒ Capturing issues in a risk register
- ☐ Executing an approved mitigation plan

Licensed to Berend Post berend.post@it-university.nl

Question 2566

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- ☒ topology diagrams.
- ☐ bandwidth usage.
- ☐ traffic analysis reports.
- ☐ bottleneck locations.

Explanation:

Explanation:

The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

Question 2567

Adding security requirements late in the software development life cycle would MOST likely result in:

- ☐ cost savings
- ☐ clearer understanding of requirements
- ☐ operational efficiency
- ☒ compensating controls

Question 2568

At a hospital, medical personal carry handheld computers which contain patient health data. These handheld computers are synchronized with PCs which transfer data from a hospital database. Which of the following would be of the most importance?

- ☒ The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
- ☐ The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
- ☐ Timely synchronization is ensured by policies and procedures.
- ☐ The usage of the handheld computers is allowed by the hospital policy.

Explanation:

Explanation:

Data confidentiality is a major requirement of privacy regulations. Choices B, C and D relate to internal security requirements, and are secondary when compared to compliance with data privacy laws.

Licensed to Berend Post berend.post@it-university.nl

Question 2569

Who is ultimately responsible for providing requirement specifications to the software- development team?

- ☒ The project sponsor
- ☐ The project members
- ☐ The project leader
- ☐ The project steering committee

Explanation:

Explanation:

The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

Question 2570

Which key is used by the sender of a message to create a digital signature for the message being sent?

- ☐ Sender's public key
- ☒ Sender's private key
- ☐ Receiver's public key
- ☐ Receiver's private key

Explanation:

The sender private key is used to calculate the digital signature

The digital signature is used to achieve integrity, authenticity and non-repudiation. In a digital signature, the sender's private key is used to encrypt the message digest (signing) of the message and receiver need to decrypt the same using sender's public key to validate the signature.

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

How It Works

Licensed to Berend Post berend.post@it-university.nl

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

You copy-and-paste the contract (it's a short one!) into an e-mail note.

Using special software, you obtain a message hash (mathematical summary) of the contract.

You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.

The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message:

To make sure it's intact and from you, your lawyer makes a hash of the received message.

Your lawyer then uses your public key to decrypt the message hash or summary.

If the hashes match, the received message is valid.

Below are some common reasons for applying a digital signature to communications:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Licensed to Berend Post berend.post@it-university.nl

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentication, non-repudiation etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purposes.

Tip for the exam:

Digital Signature does not provide confidentiality. The sender's private key is used for calculating digital signature

Encryption provides only confidentiality. The receiver's public key or symmetric key is used for encryption

The following were incorrect answers:

Sender's Public key – This is incorrect as receiver will require sender's private key to verify digital signature.

Receiver's Public Key – The digital signature provides non-repudiation. The receiver's public key is known to every one. So it can not be used for digital-signature. Receiver's public key can be used for encryption.

Receiver's Private Key – The sender does not know the receiver's private key. So this option is incorrect.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 348

http://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg

http://en.wikipedia.org/wiki/Digital_signature

Licensed to Berend Post berend.post@it-university.nl

http://searchsecurity.techtarget.com/definition/digital-signature

Question 2571

In a multinational organization, local security regulations should be implemented over global security policy because:

- ☐ global security policies include unnecessary controls for local businesses
- ☐ business objectives are defined by local business unit managers
- ☒ requirements of local regulations take precedence
- ☐ deploying awareness of local regulations is more practical than of global policy

Question 2572

What increases encryption overhead and cost the most?

- ☐ A long symmetric encryption key
- ☒ A long asymmetric encryption key
- ☐ A long Advance Encryption Standard (AES) key
- ☐ A long Data Encryption Standard (DES) key

Explanation:

Explanation:

A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys.

Question 2573

An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers-one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

- ☐ The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
- ☒ Both fire suppression systems present a risk of suffocation when used in a closed room.
- ☐ The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).
- ☐ The documentation binders should be removed from the equipment room to reduce potential risks.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Protecting people's lives should always be of highest priority in fire suppression activities. COz and halon both reduce the oxygen ratio in the atmosphere, which can induce serious personal hazards, in many countries installing or refilling halon fire suppression systems is not allowed. Although COz and halon are effective and appropriate for fires involving synthetic combustibles and electrical equipment, they are nearly totally ineffective on solid combustibles (wood and paper). Although not of highest priority, removal of the documentation would probably reduce some of the risks.

Question 2574

Implementing which of the following would BEST address issues relating to the aging of IT systems?

- ☒ IT project management
- ☐ Release management
- ☐ Application portfolio management
- ☐ Configuration management

Question 2575

During a security audit, an IS auditor is tasked with reviewing log entries obtained from an enterprise intrusion prevention system (IPS). Which type of risk would be associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration?

- ☐ Inherent risk
- ☐ Sampling risk
- ☐ Control risk
- ☒ Detection risk

Question 2576

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system’s edit routine?

- ☐ Interviews with knowledgeable users
- ☒ Use of test transactions
- ☐ Review of source code
- ☐ Review of program documentation

Licensed to Berend Post berend.post@it-university.nl

Question 2577

Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

- ☐ DTE
- ☒ DCE
- ☐ DME
- ☐ DLE

Explanation:

Data Circuit Terminal Equipment (DCE) is a service provider device that does the actual data transmission and switching in the frame relay cloud.

For your exam you should know below information about WAN Technologies:

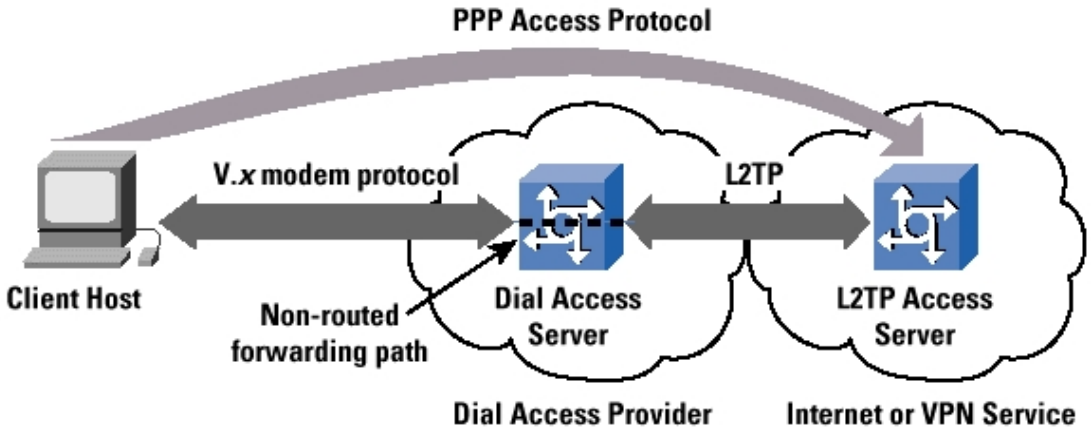
Point-to-point protocol

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Licensed to Berend Post berend.post@it-university.nl



Point-to-point protocol

X.25

X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

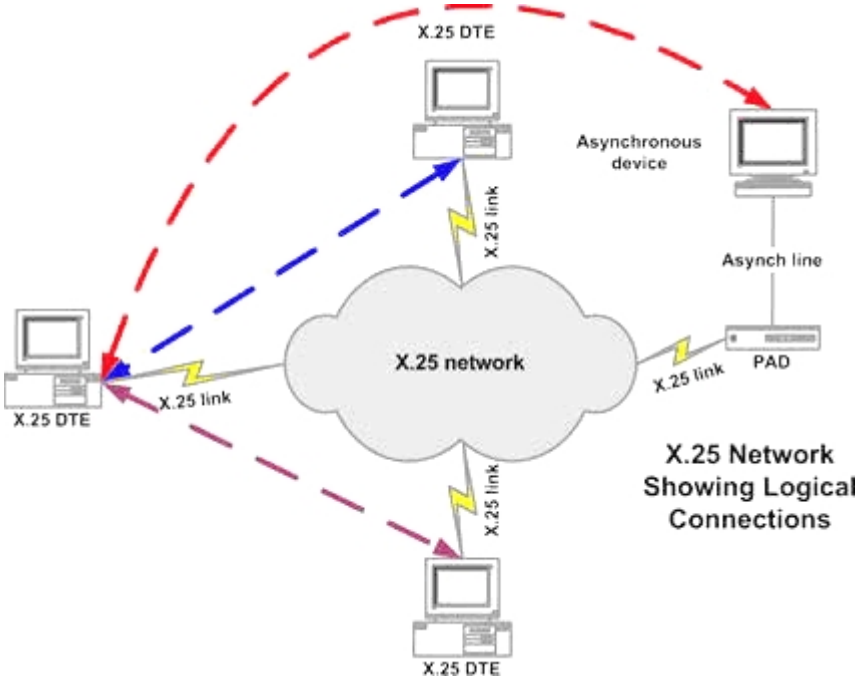
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

X.25

Licensed to Berend Post berend.post@it-university.nl



Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

Two main types of equipments are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

Frame Relay

Integrated Service Digital Network

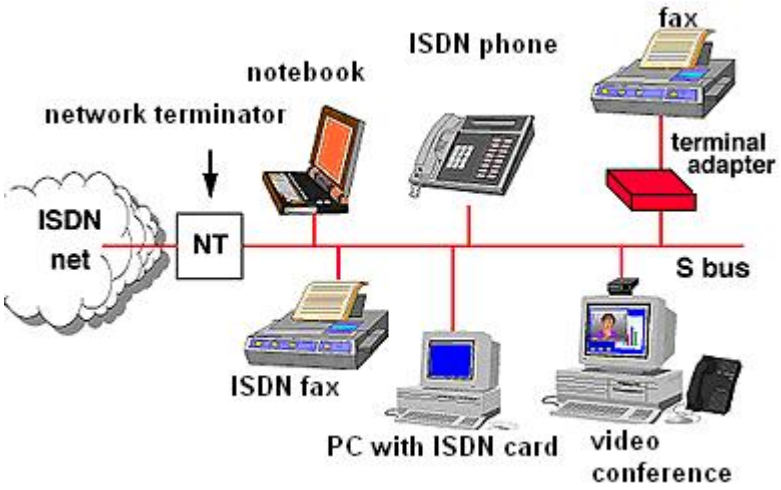
Licensed to Berend Post berend.post@it-university.nl

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium

ISDN



Asynchronous Transfer Mode (ATM)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

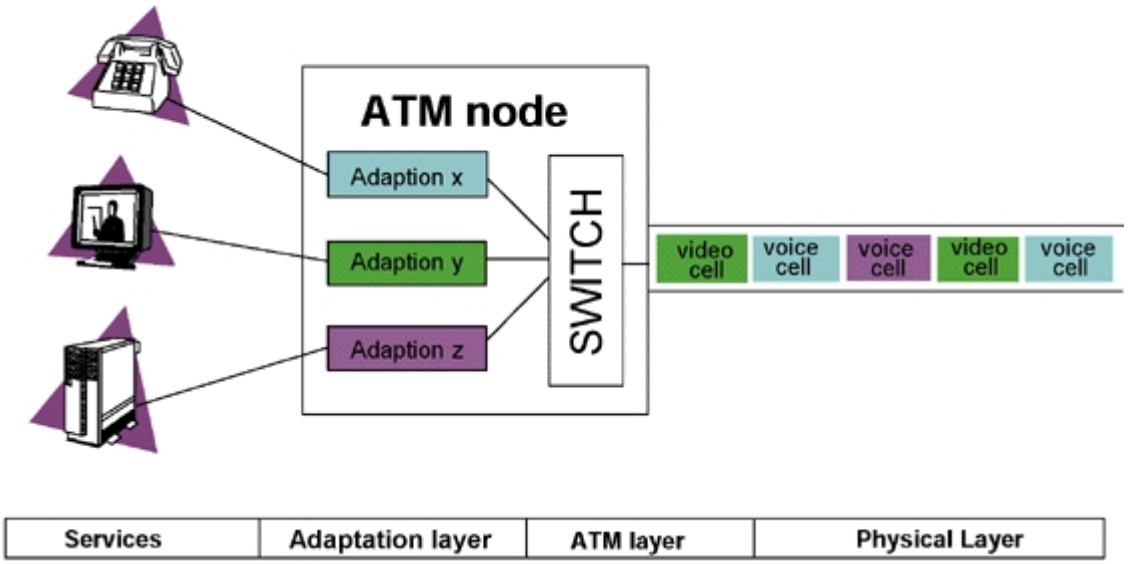
Like a frame relay it is connection oriented technology which creates and uses fixed channel

Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM

Asynchronous Transfer Mode

Licensed to Berend Post berend.post@it-university.nl

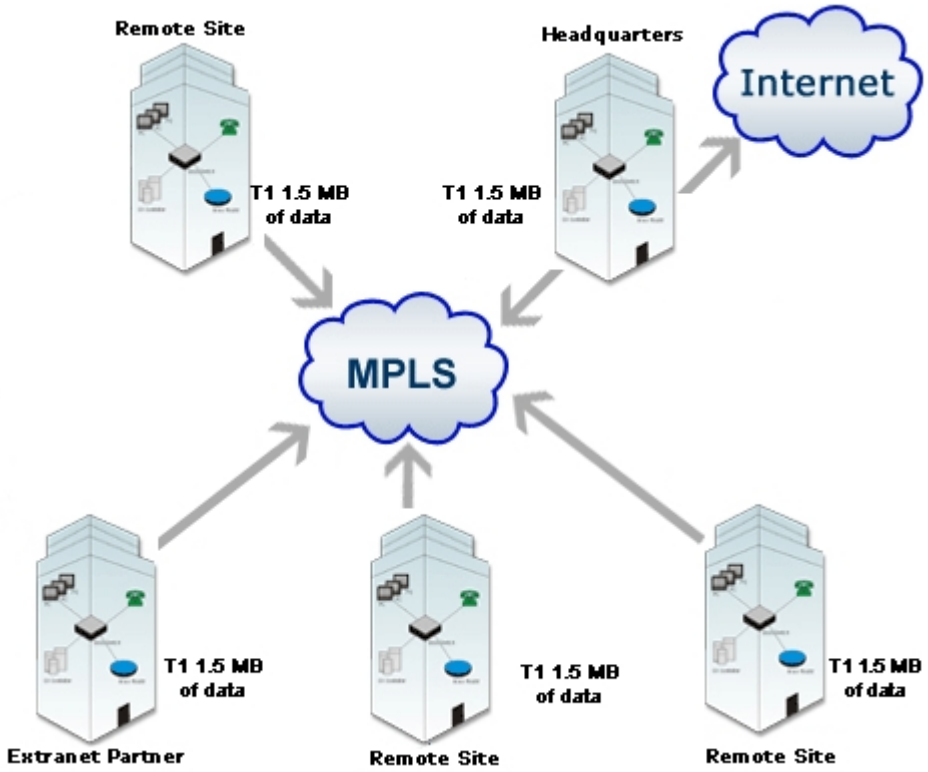


Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS

Licensed to Berend Post berend.post@it-university.nl



The following answers are incorrect:

DTE - Data Terminal Equipment (DTE) is usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

DME – Not a valid frame relay technique

DLE – Not a valid frame relay technique

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

Question 2578

Key verification is one of the best controls for ensuring that:

- ☒ Data is entered correctly
- ☐ Only authorized cryptographic keys are used
- ☐ Input is authorized
- ☐ Database indexing is performed properly

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Key verification is one of the best controls for ensuring that data is entered correctly.

Question 2579

Which of the following is the MAIN purpose of an information security management system?

- ☐ To enhance the impact of reports used to monitor information security incidents
- ☒ To reduce the frequency and impact of information security incidents
- ☐ To identify and eliminate the root causes of information security incidents
- ☐ To keep information security policies and procedures up-to-date

Question 2580

When replacing a critical software application, which of the following provides for the LOWEST risk of interruption to business processes?

- ☒ Parallel implementation
- ☐ Pilot implementation
- ☐ Incremental implementation
- ☐ Big-bang implementation

Question 2581

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- ☒ nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- ☐ access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
- ☐ card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- ☐ the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Explanation:

Explanation:

Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequate to trust unknown external people by allowing them to write down their alleged name without proof, e.g., identity card, driver's license. Choice B is not a concern because if the name and address of the organization was written on the card, a malicious finder could use the card to enter the organization's premises. Separating card issuance from technical rights management is a method to ensure a proper segregation of duties so that no single person can produce a functioning card for a restricted area within the organization's premises. Choices B and C are good practices, not concerns. Choice D may be a concern, but not as important

 Licensed to Berend Post berend.post@it-university.nl

since a system failure of the card programming device would normally not mean that the readers do not function anymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

Question 2582

A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

- ☐ Industry standards
- ☐ The business impact analysis
- ☒ The business objectives
- ☐ Previous audit recommendations

Question 2583

A lower recovery time objective (RTO) results in:

- ☐ higher disaster tolerance.
- ☒ higher cost.
- ☐ wider interruption windows.
- ☐ more permissive data loss.

Explanation:

Explanation:

A recovery time objective (RTO) is based on the acceptable downtime in case of a disruption of operations. The lower the RTO, the higher the cost of recovery strategies. The lower the disaster tolerance, the narrower the interruption windows, and the lesser the permissive data loss.

Question 2584

Which of the following would be an information security manager's PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?

- ☐ End user acceptance
- ☒ Mobile application control
- ☐ Configuration management
- ☐ Disparate device security

Licensed to Berend Post berend.post@it-university.nl

Question 2585

Which of the following technique is NOT used by a preacher against a Private Branch Exchange (PBX)?

- ☐ Eavesdropping
- ☐ Illegal call forwarding
- ☐ Forwarding a user to an unused or disabled number
- ☒ SYN Flood

Explanation:

The word NOT the keyword used in the question. You need to find out the technique which preacher do not use to exploit PBX.

SYN Flood -Sends a flood of TCP/SYN packets with forged sender address, causing half-open connections and saturates available connection capacity on the target machine.

For CISA Exam you should know below mentioned techniques used by preacher for illegal purpose of PBX.

Eavesdropping on conversation, without the other parties being aware of it

Eavesdropping on conference call

Illegal forwarding calls from specific equipment to remote numbers

Forwarding a user to an unused or disabled number, thereby making it unreachable by external calls.

The following were incorrect answers:

The other options presented correctly describes the techniques used preacher for illegal purpose of PBX.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 357

Licensed to Berend Post berend.post@it-university.nl

Question 2586

"Under the concept of ""defense in depth"", subsystems should be designed to:"

- ☐ ""fail insecure"""
- ☒ ""fail secure"""
- ☐ ""react to attack"""
- ☐ ""react to failure"""
- ☐ None of the choices.

Explanation:

Explanation:

"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure"".

Question 2587

An IS audit manager has been asked to perform a quality review on an audit that the same manager also supervised. Which of the following is the manager's BEST response to this situation?

- ☒ Notify the audit committee of the situation.
- ☐ Escalate the situation to senior audit leadership.
- ☐ Determine whether audit evidence supports audit conclusions.
- ☐ Discuss with the audit team to understand how conclusions were reached.

Question 2588

A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?

- ☒ Validity
- ☐ Existence
- ☐ Limit
- ☐ Completeness

Licensed to Berend Post berend.post@it-university.nl

Question 2589

A company requires that all program change requests (PCRs) be approved and all modifications be automatically logged. Which of the following IS audit procedures will BEST determine whether unauthorized changes have been made to production programs?

- ☐ Review a sample of PCRs for proper approval throughout the program change process.
- ☐ Trace a sample of program changes from the log to completed PCR forms.
- ☒ Use source code comparison software to determine whether any changes have been made to a sample of programs since the last audit date.
- ☐ Trace a sample of complete PCR forms to the log of all program changes.

Question 2590

The network of an organization has been the victim of several intruders' attacks. Which of the following measures would allow for the early detection of such incidents?

- ☐ Antivirus software
- ☐ Hardening the servers
- ☐ Screening routers
- ☒ Honeypots

Explanation:

Explanation:

Honeypots can collect data on precursors of attacks. Since they serve no business function, honeypots are hosts that have no authorized users other than the honeypot administrators. All activity directed at them is considered suspicious. Attackers will scan and attack honeypots, giving administrators data on new trends and attack tools, particularly malicious code. However, honeypots are a supplement to, not a replacement for, properly securing networks, systems and applications. If honeypots are to be used by an organization, qualified incident handlers and intrusion detection analysts should manage them. The other choices do not provide indications of potential attacks.

Question 2591

When reviewing a newly implemented quality management system (QMS), which of the following should be the IS auditor's PRIMARY concern?

- ☐ The QMS benefit measures were not included in the business case.
- ☐ The QMS testing methodology is not clearly documented.
- ☐ The QMS post-implementation review (PIR) has not been finalized.
- ☒ The QMS is not mapped to some core business processes.

Licensed to Berend Post berend.post@it-university.nl

Question 2592

Codes from exploit programs are frequently reused in:

- ☐ trojan horses only.
- ☐ computer viruses only.
- ☐ OS patchers.
- ☐ eavedroppers.
- ☒ trojan horses and computer viruses.
- ☐ None of the choices.

Explanation:

Explanation:

"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

Question 2593

An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

- ☒ The chain of custody has not been documented.
- ☐ The legal department has not been engaged.
- ☐ An imagining process was used to obtain a copy of the data from each computer.
- ☐ Audit was only involved during extraction of the information.

Question 2594

Which of the following metrics would BEST measure the agility of an organization's IT function?

- ☒ Average time to turn strategic IT objectives into an agreed upon and approved initiative
- ☐ Average number of learning and training hours per IT staff member
- ☐ Frequency of security assessments against the most recent standards and guidelines
- ☐ Percentage of staff with sufficient IT-related skills for the competency required of their roles.

Licensed to Berend Post berend.post@it-university.nl

Question 2595

Which of the following cloud deployment model operates solely for an organization?

- ☒ Private Cloud
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Explanation:

In Private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

For your exam you should know below information about Cloud Computing deployment models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

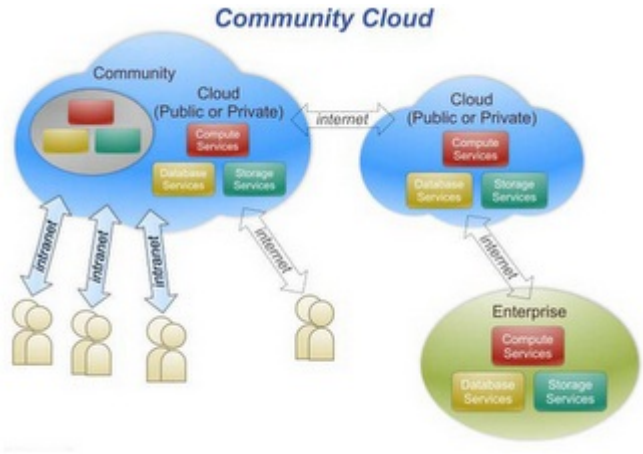
Private Cloud

Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Community Cloud

Licensed to Berend Post berend.post@it-university.nl



Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Public Cloud

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

hybrid cloud

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

Question 2596

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

- ☒ Failing to perform user acceptance testing
- ☐ Lack of user training for the new system
- ☐ Lack of software documentation and run manuals
- ☐ Insufficient unit, module, and systems testing

Explanation:

Explanation:

Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

Licensed to Berend Post berend.post@it-university.nl

Question 2597

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic entry system for a data center?

- ☒ Creates an audit trail
- ☐ Enables data mining
- ☐ Ensures compliance
- ☐ Reduces cost

Question 2598

Which of the following firewall technologies involves examining the header of every packet of data traveling between the Internet and the corporate network without examining the previous packets?

- ☐ Proxy servers
- ☐ Bastion host
- ☐ Stateful filtering
- ☒ Stateless filtering

Question 2599

Which of the following exposures could be caused by a line grabbing technique?

- ☒ Unauthorized data access
- ☐ Excessive CPU cycle usage
- ☐ Lockout of terminal polling
- ☐ Multiplexor control dysfunction

Explanation:

Explanation:

Line grabbing will enable eavesdropping, thus allowing unauthorized data access, it will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

Question 2600

Which of the following is the BEST key performance indicator (KPI) for determining how well the IT policy is aligned to the business requirements?

- ☒ Number of approved exceptions to the policy
- ☐ Total cost of policy breaches
- ☐ Total cost to support the policy
- ☐ Number of inquiries regarding the policy

Licensed to Berend Post berend.post@it-university.nl

Question 2601

Since data storage of a critical business application is on a redundant array of inexpensive disks (RAID), backups are not considered essential. The IS auditor should recommend proper backups because RAID:

- ☐ relies on proper maintenance.
- ☐ cannot offer protection against disk corruption.
- ☒ cannot recover from a natural disaster.
- ☐ disks cannot be hot-swapped for quick recovery.

Question 2602

An organization is MOST at risk from a new worm being introduced through the intranet when:

- ☐ executable code is run from inside the firewall
- ☐ system software does not undergo integrity checks
- ☐ hosts have static IP addresses
- ☒ desktop virus definition files are not up to date

Question 2603

To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

- ☐ the company policy be changed.
- ☐ passwords are periodically changed.
- ☒ an automated password management tool be used.
- ☐ security awareness training is delivered.

Explanation:

Explanation:

The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

Licensed to Berend Post berend.post@it-university.nl

Question 2604

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

- ☐ Spool
- ☐ Cluster controller
- ☐ Protocol converter
- ☒ Front end processor

Explanation:

Explanation:

A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

Question 2605

To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

- ☐ the security policy is changed to accommodate IT performance pressure
- ☐ noncompliance issues are reported senior management
- ☐ senior management provides guidance and dispute resolution
- ☒ information security management understands business performance issues

Question 2606

IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

Licensed to Berend Post berend.post@it-university.nl

Question 2607

An organization has developed mature risk management practices that are followed across all departments. What is the MOST effective way for the audit team to leverage this risk management maturity?

- ☐ Facilitating audit risk identification and evaluation workshops
- ☐ Implementing risk responses on management's behalf
- ☐ Providing assurances to management regarding risk
- ☒ Integrating the risk register for audit planning purposes

Question 2608

Which of the following would provide the STRONGEST indication that senior management commitment to information security is lacking within an organization?

- ☒ Inconsistent enforcement of information security policies
- ☐ A reduction in information security investment
- ☐ A high of information security risk acceptance
- ☐ The information security manager reports to the chief risk officer

Question 2609

Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?

- ☒ Review the business requirements document for date of birth field requirements.
- ☐ Review new account applications submitted in the past month for invalid dates of birth.
- ☐ Evaluate configuration settings for the date of birth field requirements.
- ☐ Attempt to submit new account applications with invalid dates of birth.

Question 2610

An organization has implemented a control to help ensure databases containing personal information will not be updated with online transactions that are incomplete due to connectivity issues. Which of the following information attributes is PRIMARILY addressed by this control?

- ☒ Integrity
- ☐ Confidentiality
- ☐ Availability
- ☐ Compliance

Licensed to Berend Post berend.post@it-university.nl

Question 2611

Which of the following should be done FIRSTwhen handling multiple confirmed incidents raised at the same time?

- ☒ Categorize incidents by the value of the affected asset.
- ☐ Inform senior management.
- ☐ Update the business impact assessment.
- ☐ Activate the business continuity plan.

Question 2612

When reviewing backup policies, an IS auditor MUST verify that backup intervals of critical systems do not exceed which of the following?

- ☒ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)
- ☐ Service level objective (SLO)
- ☐ Maximum acceptable outage (MAO)

Question 2613

What is the PRIMARY benefit of prototyping as a method of system development?

- ☐ Reduces the need for testing.
- ☐ Minimizes the time the IS auditor has to review the system.
- ☒ Increases the likelihood of user satisfaction.
- ☐ Eliminates the need for documentation.

Question 2614

Which of the following audit assess accuracy of financial reporting?

- ☐ Compliance Audit
- ☒ Financial Audit
- ☐ Operational Audit
- ☐ Forensic audit

Explanation:

Explanation:

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial

Licensed to Berend Post berend.post@it-university.nl

statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

For your exam you should know below information about different types of audit:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization's accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Licensed to Berend Post berend.post@it-university.nl

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Integrated Audits

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Licensed to Berend Post berend.post@it-university.nl

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance Audit - A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Operational Audit - Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives.[1] Operational audit is a more comprehensive form of an Internal audit.

Forensic Audit - Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

Licensed to Berend Post berend.post@it-university.nl

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

Question 2615

During a network security review, the system log indicates an unusually high number of unsuccessful login attempts. Which of the following sampling techniques is MOST appropriate for selecting a sample of user IDs for further investigation?

- ☒ Stratified
- ☐ Attribute
- ☐ Monetary unit
- ☐ Variable

Question 2616

Which of the following is the MOST effective control over visitor access to a data center?

- ☒ Visitors are escorted.
- ☐ Visitor badges are required.
- ☐ Visitors sign in.
- ☐ Visitors are spot-checked by operators.

Explanation:

Explanation:

Escorting visitors will provide the best assurance that visitors have permission to access the data processing facility. Choices B and C are not reliable controls. Choice D is incorrect because visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

Licensed to Berend Post berend.post@it-university.nl

Question 2617

An IS auditor finds that one employee has unauthorized access to confidential data. The IS auditor's BEST recommendation should be to:

- ☐ reclassify the data to a lower level of confidentiality.
- ☒ recommend corrective actions to be taken by the security administrator.
- ☐ implement a strong password schema for users.
- ☐ require the business owner to conduct regular access reviews.

Question 2618

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

- ☐ Schedule the target end date for implementation activities.
- ☐ Budget the total cost of implementation activities.
- ☒ Develop an implementation strategy.
- ☐ Calculate the residual risk for each countermeasure.

Question 2619

The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

- ☐ Inherent
- ☒ Detection
- ☐ Control
- ☐ Business

Explanation:

Explanation:

Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks are not usually affected by an IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by an IS auditor.

Question 2620

Which of the following best characterizes "worms"?

- ☒ Malicious programs that can run independently and can propagate without the aid of a carrier program such as email.
- ☐ Programming code errors that cause a program to repeatedly dump data
- ☐ Malicious programs that require the aid of a carrier program such as email
- ☐ Malicious programs that masquerade as common applications such as screensavers or macro- enabled Word documents

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Worms are malicious programs that can run independently and can propagate without the aid of a carrier program such as email.

Question 2621

What are used as the framework for developing logical access controls?

- ☒ Information systems security policies
- ☐ Organizational security policies
- ☐ Access Control Lists (ACL)
- ☐ Organizational charts for identifying roles and responsibilities

Explanation:

Explanation:

Information systems security policies are used as the framework for developing logical access controls.

Question 2622

Which of the following security risks can be reduced by a properly configured network firewall?

- ☐ Insider attacks
- ☐ SQL injection attacks
- ☒ Denial of service (DoS) attacks
- ☐ Phishing attacks

Question 2623

As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and system from the organization being acquired into existing systems. To ensure the data is relevant, the acquiring organization should:

- ☐ obtain data quality software.
- ☒ define data quality requirements based on business needs.
- ☐ automate the process of data collection and cleaning.
- ☐ implement a data warehouse solution.

Licensed to Berend Post berend.post@it-university.nl

Question 2624

Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

- ☐ A hot site maintained by the business
- ☐ A commercial cold site
- ☒ A reciprocal arrangement between its offices
- ☐ A third-party hot site

Explanation:

Explanation:

For a business having many offices within a region, a reciprocal arrangement among its offices would be most appropriate. Each office could be designated as a recovery site for some other office. This would be the least expensive approach to providing an acceptable level of confidence. A hot site maintained by the business would be a costly solution but would provide a high degree of confidence. Multiple cold sites leased for the multiple offices would lead to a costly solution with a high degree of confidence. A third-party facility for recovery is provided by a traditional hot site. This would be a costly approach providing a high degree of confidence.

Question 2625

Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem?

- ☐ Expert systems
- ☒ Neural networks
- ☐ Integrated synchronized systems
- ☐ Multitasking applications

Explanation:

Explanation:

Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

Question 2626

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

- ☐ not be concerned since there may be other compensating controls to mitigate the risks.
- ☒ ensure that overrides are automatically logged and subject to review.
- ☐ verify whether all such overrides are referred to senior management for approval.
- ☐ recommend that overrides not be permitted.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. As long as the overrides are policy- compliant, there is no need for senior management approval or a blanket prohibition.

Question 2627

Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

- ☐ An emerging technologies strategy would be in place
- ☐ A cost-benefit analysis process would be easier to perform
- ☒ An effective security risk management process is established
- ☐ End-user acceptance of emerging technologies has been established

Question 2628

Assessing IT risks is BEST achieved by:

- ☒ evaluating threats associated with existing IT assets and IT projects.
- ☐ using the firm's past actual loss experience to determine current exposure.
- ☐ reviewing published loss statistics from comparable organizations.
- ☐ reviewing IT control weaknesses identified in audit reports.

Explanation:

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

Licensed to Berend Post berend.post@it-university.nl

Question 2629

The operations team of an organization has reported an IS security attack. Which of the following should be the NEXT step for the security incident response team?

- ☐ Document lessons learned.
- ☒ Prioritize resources for corrective action.
- ☐ Perform a damage assessment.
- ☐ Report results to management.

Question 2630

Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

- ☐ Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
- ☐ Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables.
- ☒ Extrapolation of the overall end date based on completed work packages and current resources
- ☐ Calculation of the expected end date based on current resources and remaining available project budget

Explanation:

Explanation:

Direct observation of results is better than estimations and qualitative information gained from interviews or status reports. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

Question 2631

Following best practices, formal plans for implementation of new information systems are developed during the:

- ☐ development phase.
- ☒ design phase.
- ☐ testing phase.
- ☐ deployment phase.

Explanation:

Explanation:

Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

Licensed to Berend Post berend.post@it-university.nl

Question 2632

An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

- ☐ report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
- ☐ verify that user access rights have been granted on a need-to-have basis.
- ☒ recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
- ☐ recommend that activity logs of terminated users be reviewed on a regular basis.

Explanation:

Explanation:

Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate, the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted.

Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

Question 2633

During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

- ☒ Eradication
- ☐ Identification
- ☐ Review
- ☐ Containment

Licensed to Berend Post berend.post@it-university.nl

Question 2634

While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

- ☒ requirement for protecting confidentiality of information could be compromised.
- ☐ contract may be terminated because prior permission from the outsourcer was not obtained.
- ☐ other service provider to whom work has been outsourced is not subject to audit.
- ☐ outsourcer will approach the other service provider directly for further work.

Explanation:

Explanation:

Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are no related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

Question 2635

Which of the following should be a concern to an IS auditor reviewing a wireless network?

- ☐ 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
- ☒ SSID (Service Set IDentifier) broadcasting has been enabled.
- ☐ Antivirus software has been installed in all wireless clients.
- ☐ MAC (Media Access Control) access control filtering has been deployed.

Explanation:

Explanation:

SSID broadcasting allows a user to browse for available wireless networks and to access them without authorization. Choices A, C and D are used to strengthen a wireless network.

Question 2636

An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to- disk solution. This is appropriate because:

- ☒ fast synthetic backups for offsite storage are supported.
- ☐ backup to disk is always significantly faster than backup to tape.
- ☐ tape libraries are no longer needed.
- ☐ data storage on disks is more reliable than on tapes.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Disk-to-disk (D2D) backup should not be seen as a direct replacement for backup to tape; rather, it should be viewed as part of a multitier backup architecture that takes advantage of the best features of both tape and disk technologies. Backups to disks are not dramatically faster than backups to tapes in a balanced environment. Most often than not there is hardly a difference, since the limiting components are not tape or disk drives but the overall sustained bandwidth of the backup server's backplane. The advantage in terms of speed is in restoring performance, since all data are on hand and can be accessed randomly, resulting in a dramatic enhancement in throughput. This makes fast synthetic backups (making a full back up without touching the host's data only by using the existing incremental backups) efficient and easy. Although the cost of disks has been reduced, tape-based backup can offer an overall cost advantage over disk-only solutions. Even if RAID arrays are used for D2Dstorage, a failed drive must be swapped out and the RAID set rebuilt before another disk drive fails, thus making this kind of backup more risky and not suitable as a solution of last resort. In contrast, a single tape drive failure does not produce any data loss since the data resides on the tape media. In a multidrive library, the loss of the use of a single tape drive has no impact on the overall level of data protection. Conversely, the loss of a disk drive in an array can put all data at risk. This in itself reinforces the benefits of a disk-to-disk-to-any storage hierarchy, as data could be protected by a tertiary stage of disk storage and ultimately tape. Beyond the drive failure issue, tape has an inherent reliability advantage over any disk drive as it has no boot sector or file allocation table that can be infected or manipulated by a virus.

Question 2637

A user of a telephone banking system has forgotten his personal identification number (PIN). After the user has been authenticated, the BEST method of issuing a new PIN is to have:

- ☒ the user enter a new PIN twice.
- ☐ banking personnel verbally assign a new PIN.
- ☐ a randomly generated PIN communicated by banking personnel.
- ☐ banking personnel assign the user a new PIN via email.

Question 2638

The development of an IS security policy is ultimately the responsibility of the:

- ☐ IS department.
- ☐ security committee.
- ☐ security administrator.
- ☒ board of directors.

Explanation:

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for

 Licensed to Berend Post berend.post@it-university.nl

implementing, monitoring and enforcing the security rules that management has established and authorized.

Question 2639

During an external assessment of network vulnerability, which of the following activities should be performed FIRST?

- ☒ Collect network information
- ☐ Implement an intrusion detection system (IDS)
- ☐ Monitor the network
- ☐ Review policies

Question 2640

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- ☒ Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan.
- ☐ Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
- ☐ No, because the backup to be provided should be specified adequately in the contract.
- ☐ No, because the service bureau's business continuity plan is proprietary information.

Explanation:

Explanation:

The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

Question 2641

What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

- ☐ Contrived data
- ☐ Independently created data
- ☐ Live data
- ☒ Data from previous tests

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

Question 2642

Which of the following transmission media is MOST difficult to tap?

- ☐ Copper cable
- ☒ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Radio System

Explanation:

Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

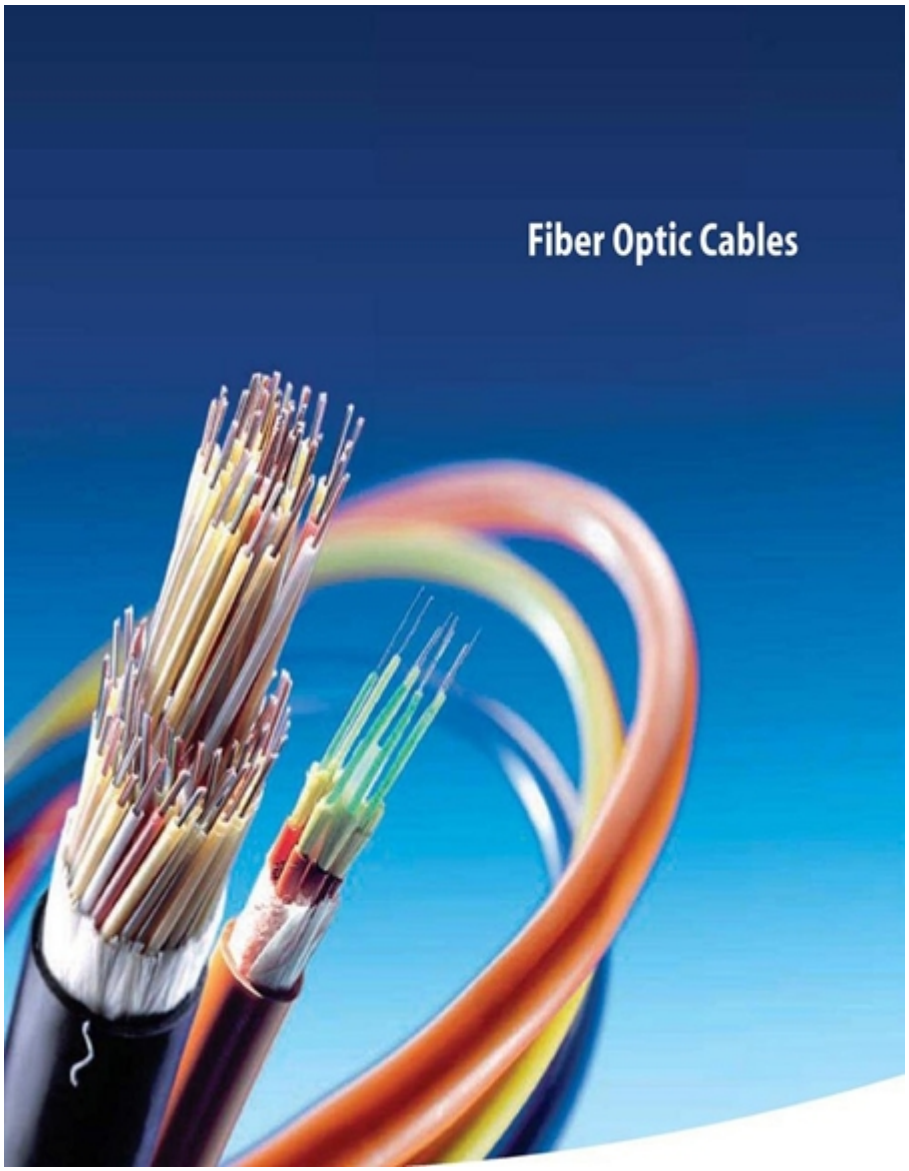
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Licensed to Berend Post berend.post@it-university.nl

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum

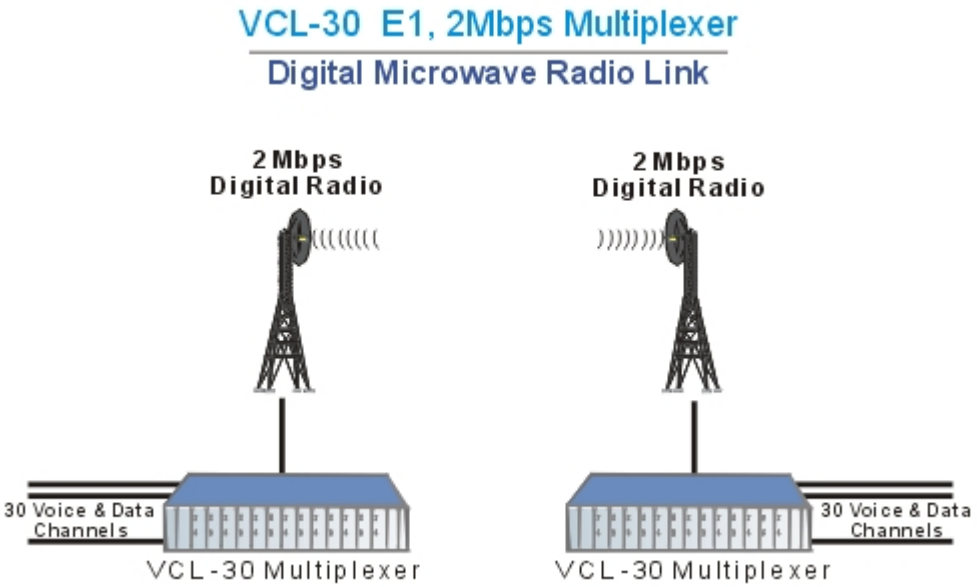
Licensed to Berend Post berend.post@it-university.nl

below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Licensed to Berend Post berend.post@it-university.nl

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265

Question 2643

Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation? Computers on the network that are located:

- ☐ on the enterprise's internal network.
- ☐ at the backup site.
- ☒ in employees' homes.
- ☐ at the enterprise's remote offices.

Explanation:

Explanation:

One risk of a virtual private network (VPN) implementation is the chance of allowing high- risk computers onto the enterprise's network. All machines that are allowed onto the virtual network should be subject to the same security policy. Home computers are least subject to the corporate security policies, and therefore are high-risk computers. Once a computer is hacked and 'owned/ any network that trusts that computer is at risk. Implementation and adherence to corporate security policy is easier when all computers on the network are on the enterprise's campus. On an enterprise's internal network, there should be security policies in place to detect and halt an outside attack that uses an internal machine as a staging platform. Computers at the backup site are subject to the corporate security policy, and therefore are not high-risk computers. Computers on the network that are at the enterprise's remote offices, perhaps with different IS and security employees who have different ideas about security, are more risky than choices A and B, but obviously less risky than home computers.

 Licensed to Berend Post berend.post@it-university.nl

Question 2644

In an organization where IT is critical to its business strategy and where there is a high level of operational dependence on IT, senior management commitment to security is BEST demonstrated by the:

- ☐ reporting line of the chief information security officer (CISO).
- ☐ segregation of duties policy.
- ☒ existence of an IT steering committee.
- ☐ size of the IT security function.

Question 2645

To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

- ☒ Include strategic objectives in IT staff performance objectives.
- ☐ Review IT staff job descriptions for alignment.
- ☐ Identify required IT skill sets that support key business processes.
- ☐ Develop quarterly training for each IT staff member.

Question 2646

An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the FIRST control required before implementation?

- ☐ Device baseline configurations
- ☒ Device registration
- ☐ An acceptable use policy
- ☐ An awareness program

Question 2647

An organization's disposal policy emphasizes obtaining maximum value for surplus IT media. The IS auditor should obtain assurance that:

- ☐ the media is returned to the vendor for credit
- ☐ any existing data is removed before disposal
- ☐ identification labels are removed
- ☒ the media is recycled to other groups within the organization

Licensed to Berend Post berend.post@it-university.nl

Question 2648

Which of the following control is intended to discourage a potential attacker?

- ☒ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Explanation:

Explanation:

Deterrent Control are intended to discourage a potential attacker

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Licensed to Berend Post berend.post@it-university.nl

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be

Licensed to Berend Post berend.post@it-university.nl

established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Preventive - Preventive controls are intended to avoid an incident from occurring

 Licensed to Berend Post berend.post@it-university.nl

Corrective - Corrective control fixes components or systems after an incident has occurred

Recovery - Recovery controls are intended to bring the environment back to regular operations

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 2649

Which of the following malware technical fool's malware by appending section of themselves to files – somewhat in the same way that file malware appends themselves?

- ☐ Scanners
- ☐ Active Monitors
- ☒ Immunizer
- ☐ Behavior blocker

Explanation:

Immunizers defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

For your exam you should know below mentioned different kinds of malware Controls

A. Scanners- Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

 Licensed to Berend Post berend.post@it-university.nl

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker- Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

E. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

The following were incorrect answers:

Scanners -Look for sequences of bit called signature that are typical malware programs.

Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between

 Licensed to Berend Post berend.post@it-university.nl

a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Behavior Blocker- Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 354 and 355

Question 2650

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- ☐ are developed for the organization as a whole
- ☒ are more likely to be derived as a result of a risk assessment.
- ☐ will not conflict with overall corporate policy.
- ☐ ensure consistency across the organization.

Explanation:

Explanation:

A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

Question 2651

A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

- ☐ Most employees use laptops.
- ☐ A packet filtering firewall is used.
- ☐ The IP address space is smaller than the number of PCs.
- ☒ Access to a network port is not restricted.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Given physical access to a port, anyone can connect to the internal network. The other choices do not present the exposure that access to a port does. DHCP provides convenience (an advantage) to the laptop users. Sharing IP addresses and the existence of a firewall can be security measures.

Question 2652

Which of the following functionality is NOT supported by SSL protocol?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Authentication
- ☒ Availability

Explanation:

The NOT is a keyword used in this question. You need to find out the functionality which is NOT provided by SSL protocol. The SSL protocol provides:

Confidentiality

Integrity

Authentication, e.g. between client and server

Non-repudiation

For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)

These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases

Peer negotiation for algorithm support

Public-key, encryption based key exchange and certificate based authentication

Licensed to Berend Post berend.post@it-university.nl

Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

Confidentiality - It is supported by the SSL Protocol

Integrity -It is supported by the SSL Protocol

Authentication - It is supported by the SSL protocol

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 352

Question 2653

An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

- ☐ critical
- ☐ vital.
- ☒ sensitive.
- ☐ noncritical.

Explanation:

Explanation:

Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time; this is associated with

Licensed to Berend Post berend.post@it-university.nl

lower costs of disruption than critical functions. Noncritical functions may be interrupted for an extended period of time at little or no cost to the company, and require little time or cost to restore.

Question 2654

While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed with the audit function. In order to resolve the situation, the IS auditor's BEST course of action would be to:

- ☒ determine whether the alternative controls sufficiently mitigate the risk and record the results.
- ☐ reject the alternative controls and re-prioritize the original issue as high risk.
- ☐ postpone follow-up activities and escalate the alternative controls to senior audit management.
- ☐ schedule another audit due to the implementation of alternative controls.

Question 2655

Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?

- ☐ Users should not leave tokens where they could be stolen
- ☐ Users must never keep the token in the same bag as their laptop computer
- ☐ Users should select a PIN that is completely random, with no repeating digits
- ☒ Users should never write down their PIN

Explanation:

Explanation:

If a user writes their PIN on a slip of paper, an individual with the token, the slip of paper, and the computer could access the corporate network. A token and the PIN is a two-factor authentication method. Access to the token is of no value without the PIN; one cannot work without the other. The PIN does not need to be random as long as it is secret.

Question 2656

_____ should be implemented as early as data preparation to support data integrity at the earliest point possible.

- ☒ Control totals
- ☐ Authentication controls
- ☐ Parity bits
- ☐ Authorization controls

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Control totals should be implemented as early as data preparation to support data integrity at the earliest point possible.

Question 2657

Which of the following controls would BEST decrease the exposure if a password is compromised?

- ☐ Passwords are masked.
- ☐ Passwords are encrypted.
- ☐ Passwords have format restrictions.
- ☒ Password changes are forced periodically.

Question 2658

Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

- ☐ Analyzer
- ☐ Administration console
- ☐ User interface
- ☒ Sensor

Explanation:

Explanation:

Sensors are responsible for collecting data. Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

Question 2659

Based on the guidance of internal audit, an IT steering committee is considering the use of a balanced scorecard to evaluate its project management process. Which of the following is the GREATEST advantage to using this approach?

- ☐ Project schedule and budget management will improve.
- ☒ Performance is measured from different perspectives.
- ☐ Information is provided in a consistent and timely manner.
- ☐ Project will be prioritized based on value.

Licensed to Berend Post berend.post@it-university.nl

Question 2660

Which of the following functions is performed by a virtual private network (VPN)?

- ☒ Hiding information from sniffers on the net
- ☐ Enforcing security policies
- ☐ Detecting misuse or mistakes
- ☐ Regulating access

Explanation:

Explanation:

A VPN hides information from sniffers on the net using encryption. It works based on tunneling. A VPN does not analyze information packets and, therefore, cannot enforce security policies, it also does not check the content of packets, so it cannot detect misuse or mistakes. A VPN also does not perform an authentication function and, therefore, cannot regulate access.

Question 2661

A company is using a software developer for a project. At which of the following points should the software quality assurance (QA) plan be developed?

- ☐ As part of software definition
- ☐ During the feasibility phase
- ☐ Prior to acceptance testing
- ☒ As part of the design phase

Question 2662

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- ☐ avoidance
- ☐ transference
- ☒ mitigation
- ☐ acceptance

Explanation:

Explanation:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

Licensed to Berend Post berend.post@it-university.nl

Question 2663

An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

- ☐ provides authenticity.
- ☐ is faster than asymmetric encryption.
- ☒ can cause key management to be difficult.
- ☐ requires a relatively simple algorithm.

Explanation:

Explanation:

In a symmetric algorithm, each pair of users' needs a unique pair of keys, so the number of keys grows and key management can become overwhelming. Symmetric algorithms do not provide authenticity, and symmetric encryption is faster than asymmetric encryption. Symmetric algorithms require mathematical calculations, but they are not as complex as asymmetric algorithms.

Question 2664

Which of the following should be reviewed FIRST when planning an IS audit?

- ☐ Recent financial information
- ☐ Annual business unit budget
- ☐ IS audit standards
- ☒ The business environment

Question 2665

Which of the following is the MOST effective means of helping management and the IT strategy committee to monitor IT performance?

- ☐ End-user satisfaction surveys
- ☐ Gap analysis
- ☒ Measurement of service levels against metrics
- ☐ Infrastructure monitoring reports

Question 2666

During an audit of identity and access management, an IS auditor finds that the engagement audit plan does not include the testing of controls that regulate access by third parties. Which of the following would be the auditor's BEST course of action?

- ☐ Plan to test these controls in another audit.
- ☐ Escalate the deficiency to audit management.
- ☐ Add testing of third-party access controls to the scope of the audit.
- ☒ Determine whether the risk has been identified in the planning documents.

Licensed to Berend Post berend.post@it-university.nl

Question 2667

What is the MOST important business concern when an organization is about to migrate a mission-critical application to a virtual environment?

- ☐ The organization's experience with virtual applications
- ☐ Adequacy of the fallback procedures
- ☐ Confidentiality of network traffic
- ☒ Adequacy of the virtual architecture

Question 2668

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- ☐ User management coordination does not exist.
- ☐ Specific user accountability cannot be established.
- ☒ Unauthorized users may have access to originate, modify or delete data.
- ☐ Audit recommendations may not be implemented.

Explanation:

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

Question 2669

Which of the following ACID property in DBMS ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other?

- ☐ Atomicity
- ☐ Consistency
- ☒ Isolation
- ☐ Durability

Explanation:

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must

Licensed to Berend Post berend.post@it-university.nl

guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction. [citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

The following were incorrect answers:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 Page number 218

Question 2670

Establishing data ownership is an important first step for which of the following processes?

- ☐ Assigning user access privileges
- ☐ Developing organizational security policies
- ☐ Creating roles and responsibilities
- ☒ Classifying data

Explanation:

Explanation:

To properly implement data classification, establishing data ownership is an important first step.

Question 2671

While conducting a test of a business continuity plan, which of the following is the MOST important consideration?

- ☒ The test simulates actual prime-time processing conditions.
- ☐ The test is scheduled to reduce operational impact.
- ☐ The test involves IT members in the test process.
- ☐ The test addresses the critical components.

Question 2672

Which of the following audit techniques is MOST appropriate for verifying application program controls?

- ☐ Statistical sampling
- ☐ Code review
- ☐ Confirmation of accounts
- ☒ Use of test data

Question 2673

Which of the following types of spyware was originally designed for determining the sources of error or for measuring staff productivity?

- ☐ Keywords logging
- ☒ Keystroke logging
- ☐ Directory logging
- ☐ Password logging
- ☐ None of the choices.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Keystroke logging (in the form of spyware) was originally a function of diagnostic tool deployed by software developers for capturing user's keystrokes.

This is done for determining the sources of error or for measuring staff productivity.

Question 2674

Which of the following would BEST detect that a distributed-denial-of-service attack (DDoS) is occurring?

- ☐ Server crashes
- ☒ Automated monitoring of logs
- ☐ Penetration testing
- ☐ Customer service complaints

Question 2675

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

- ☐ confirm that the auditors did not overlook any important issues.
- ☒ gain agreement on the findings.
- ☐ receive feedback on the adequacy of the audit procedures.
- ☐ test the structure of the final presentation.

Explanation:

Explanation:

The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

Question 2676

An organization is considering whether to allow employees to use personal computing devices for business purposes. To BEST facilitate senior management's decision, the information security manager should:

- ☐ perform a cost-benefit analysis
- ☒ map the strategy to business objectives
- ☐ conduct a risk assessment
- ☐ develop a business case

Licensed to Berend Post berend.post@it-university.nl

Question 2677

An application development team is also promoting changes to production for a critical financial application. Which of the following would be the BEST control to reduce the associated risk?

- ☒ Implementing a change management code review
- ☐ Implementing a peer review process
- ☐ Performing periodic audits
- ☐ Submitting change logs to the business manager for review

Question 2678

The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

- ☐ data integrity.
- ☐ authentication.
- ☒ non repudiation.
- ☐ replay protection.

Explanation:

Explanation:

All of the above are features of a digital signature. Non repudiation ensures that the claimed sender cannot later deny generating and sending the message. Data integrity refers to changes in the plaintext message that would result in the recipient failing to compute the same message hash. Since only the claimed sender has the key, authentication ensures that the message has been sent by the claimed sender. Replay protection is a method that a recipient can use to check that the message was not intercepted and replayed.

Question 2679

The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- ☒ make unauthorized changes to the database directly, without an audit trail.
- ☐ make use of a system query language (SQL) to access information.
- ☐ remotely access the database.
- ☐ update data without authentication.

Explanation:

Explanation:

Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information, in a networked environment, accessing the database remotely does not make a difference.

What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user ID.

Licensed to Berend Post berend.post@it-university.nl

Question 2680

What is the PRIMARY reason for hardening new devices before introducing into a corporate network?

- ☐ To comply with organizational rules
- ☐ To ease maintenance of devices
- ☒ To reduce exposure to attacks
- ☐ To avoid software licensing conflicts

Question 2681

The control that MOST effectively addresses the risk of piggybacking/tailgating into a restricted area without a dead man door is:

- ☐ using biometric door locks.
- ☒ security awareness training.
- ☐ requiring employees to wear ID badges.
- ☐ using two-factor authentication.

Question 2682

What supports data transmission through split cable facilities or duplicate cable facilities?

- ☒ Diverse routing
- ☐ Dual routing
- ☐ Alternate routing
- ☐ Redundant routing

Explanation:

Explanation: Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

Question 2683

A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

- ☐ Badge readers are installed in locations where tampering would be noticed
- ☐ The computer that controls the badge system is backed up frequently
- ☒ A process for promptly deactivating lost or stolen badges exists
- ☐ All badge entry attempts are logged

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Tampering with a badge reader cannot open the door, so this is irrelevant. Logging the entry attempts may be of limited value. The biggest risk is from unauthorized individuals who can enter the data center, whether they are employees or not. Thus, a process of deactivating lost or stolen badges is important. The configuration of the system does not change frequently, therefore frequent backup is not necessary.

Question 2684

Which of the following is MOST important when an organization contracts for the long-term use of a custom-developed application?

- ☐ Documented coding standards
- ☐ Error correction management
- ☒ Contract renewal provisions
- ☐ Escrow clause

Question 2685

Which of the following type of computer has highest processing speed?

- ☒ Supercomputers
- ☐ Midrange servers
- ☐ Personal computers
- ☐ Thin client computers

Explanation:

Supercomputers are very large and expensive computers with the highest processing speed, designed to be used for specialized purpose or fields that require extensive processing power.

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations.

A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS.

An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers

A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user

Licensed to Berend Post berend.post@it-university.nl

with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Laptop computers

A laptop is a portable personal computer with a clamshell form factor, suitable for mobile use.[1] They are also sometimes called notebook computers or notebooks. Laptops are commonly used in a variety of settings, including work, education, and personal multimedia.

A laptop combines the components and inputs as a desktop computer; including display, speakers, keyboard, and pointing device (such as a touchpad), into a single device. Most modern-day laptop computers also have a webcam and a mice (microphone) pre-installed. [citation needed] A laptop can be powered either from a rechargeable battery, or by mains electricity via an AC adapter. Laptops are a diverse category of devices, and other more specific terms, such as ultra-books or net books, refer to specialist types of laptop which have been optimized for certain uses. Hardware specifications change vastly between these classifications, forgoing greater and greater degrees of processing power to reduce heat emissions.

Smartphone, tablets and other handheld devices

A mobile device (also known as a handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard.

A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

Early pocket-sized devices were joined in the late 2000s by larger but otherwise similar tablet computers. Much like in a personal digital assistant (PDA), the input and output of modern mobile devices are often combined into a touch-screen interface.

Smartphone's and PDAs are popular amongst those who wish to use some of the powers of a conventional computer in environments where carrying one would not be practical. Enterprise digital assistants can further extend the available functionality for the business user by offering integrated data capture devices like barcode, RFID and smart card readers.

Thin Client computers

Licensed to Berend Post berend.post@it-university.nl

A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following answers are incorrect:

Mid-range servers- Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM).

Personal computers - A personal computer (PC) is a general-purpose computer, whose size, capabilities and original sale price makes it useful for individuals, and which is intended to be operated directly by an end-user with no intervening computer operator. This contrasted with the batch processing or time-sharing models which allowed larger, more expensive minicomputer and mainframe systems to be used by many people, usually at the same time. Large data processing systems require a full-time staff to operate efficiently.

Thin Client computers- A thin client (sometimes also called a lean, zero or slim client) is a computer or a computer program that depends heavily on some other computer (its server) to fulfill its computational roles. This is different from the traditional fat client, which is a computer designed to take on these roles by itself. The specific roles assumed by the server may vary, from providing data persistence (for example, for diskless nodes) to actual information processing on the client's behalf.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 246

http://en.wikipedia.org/wiki/Thin_client

http://en.wikipedia.org/wiki/Mobile_device

http://en.wikipedia.org/wiki/Personal_computer

http://en.wikipedia.org/wiki/Classes_of_computers

http://en.wikipedia.org/wiki/Laptop

 Licensed to Berend Post berend.post@it-university.nl

Question 2686

In the IT department where segregation of duties is not feasible due to a limited number of resources, a team member is performing the functions of computer operator and reviewer of application logs. Which of the following would be the IS auditor's BEST recommendation?

- ☒ Develop procedures to verify that the application logs are not modified.
- ☐ Prevent the operator from performing application development activities.
- ☐ Assign an independent second reviewer to verify the application logs.
- ☐ Restrict the computer operator's access to the production environment.

Question 2687

Which of the following presents an inherent risk with no distinct identifiable preventive controls?

- ☐ Piggybacking
- ☐ Viruses
- ☒ Data diddling
- ☐ Unauthorized application shutdown

Explanation:

Explanation:

Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-re plicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdown of an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

Licensed to Berend Post berend.post@it-university.nl

Question 2688

Which of the following fourth generation language depends on self-contained database management systems?

- ☐ Query and report generator
- ☒ Embedded database 4GLs
- ☐ Relational database 4GL
- ☐ Application generators

Explanation:

Embedded database 4GLsare depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

For CISA exam you should know below mentioned types of 4GLs

Query and report generator – These specialize language can extract and produce reports. Recently more powerful language has been produced that can access database records, produce complex on-line output and be developed in an almost natural language.

Embedded database 4GLs – These depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line. These allow the application developer to make better use of DBMS product, but they often are not end-user-oriented. Example include SQL+ MANTIS and NATURAL.

Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.

The following were incorrect answers:

Query and report generator – These specialize language can extract and produce reports.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line.

Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C.

Licensed to Berend Post berend.post@it-university.nl

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 209

Question 2689

An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

- ☐ apply the patch according to the patch's release notes.
- ☒ ensure that a good change management process is in place.
- ☐ thoroughly test the patch before sending it to production.
- ☐ approve the patch after doing a risk assessment.

Explanation:

Explanation:

An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly. The other choices are part of a good change management process but are not an IS auditor's responsibility.

Question 2690

The use of a GANTT chart can:

- ☒ aid in scheduling project tasks.
- ☐ determine project checkpoints.
- ☐ ensure documentation standards.
- ☐ direct the post-implementation review.

Explanation:

Explanation:

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

Licensed to Berend Post berend.post@it-university.nl

Question 2691

What kind of testing should programmers perform following any changes to an application or system?

- ☒ Unit, module, and full regression testing
- ☐ Module testing
- ☐ Unit testing
- ☐ Regression testing

Explanation:

Explanation:

Programmers should perform unit, module, and full regression testing following any changes to an application or system.

Question 2692

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- ☒ include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
- ☐ not include the finding in the final report, because the audit report should include only unresolved findings.
- ☐ not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
- ☐ include the finding in the closing meeting for discussion purposes only.

Explanation:

Explanation:

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

Question 2693

Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

- ☒ Multiple cycles of backup files remain available.
- ☐ Access controls establish accountability for e-mail activity.
- ☐ Data classification regulates what information should be communicated via e-mail.
- ☐ Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

Question 2694

Common implementations of strong authentication may use which of the following factors in their authentication efforts (Choose three.):

- ☒ 'something you know'
- ☒ 'something you have'
- ☒ 'something you are'
- ☐ 'something you have done in the past on this same system'
- ☐ 'something you have installed on this same system'
- ☐ None of the choices.

Explanation:

Explanation:

Two-factor authentication (T-FA) refers to any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as the other factor. In fact, using more than one factor is also called strong authentication. On the other hand, using just one factor is considered by some weak authentication.

Question 2695

Which of the following is MOST effective against system intrusions?

- ☐ Continuous monitoring
- ☒ Layered protection
- ☐ Penetration testing
- ☐ Two-factor authentication

Licensed to Berend Post berend.post@it-university.nl

Question 2696

Which of the following is BEST addressed when using a timestamp within a digital signature to deliver sensitive financial information?

- ☒ Replay protection
- ☐ Authentication
- ☐ Nonrepudiation
- ☐ Data integrity

Question 2697

Which of the following will BEST ensure that a proper cutoff has been established to reinstate transactions and records to their condition just prior to a computer system failure?

- ☐ Maintaining system console logs in electronic format
- ☐ Ensuring bisynchronous capabilities on all transmission lines
- ☒ Using a database management system (DBMS) to dynamically back-out partially processed transactions
- ☐ Rotating backup copies of transaction files offsite

Question 2698

Which of the following term related to network performance refers to the actual rate that information is transferred over a network?

- ☐ Bandwidth
- ☒ Throughput
- ☐ Latency
- ☐ Jitter

Explanation:

Throughput the actual rate that information is transferred. In data transmission, throughput is the amount of data moved successfully from one place to another in a given time period.

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Licensed to Berend Post berend.post@it-university.nl

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

The following reference(s) were/was used to create this question:

 Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 page number 275

Question 2699

Which of the following roles should be PRIMARILY responsible for assigning sensitivity levels to an organization's financial and payroll databases?

- ☐ Information security manager
- ☒ Data owner
- ☐ Systems administrator
- ☐ Database administrator

Question 2700

An organization allows employees to use personally owned mobile devices to access customers' personal information. An IS auditor's GREATEST concern should be whether:

- ☐ mobile devices are compatible with company infrastructure.
- ☐ devices have the capability to segregate business and personal data.
- ☒ mobile device security policies have been implemented.
- ☐ devices have adequate storage and backup capabilities.

Question 2701

Which of the following is NOT a true statement about public key infrastructure (PKI)?

- ☒ The Registration authority role is to validate and issue digital certificates to end users
- ☐ The Certificate authority role is to issue digital certificates to end users
- ☐ The Registration authority (RA) acts as a verifier for Certificate Authority (CA)
- ☐ Root certificate authority's certificate is always self-signed

Explanation:

The word NOT is the keyword used in the question. We need to find out the invalid statement from the options.

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message. Traditional

Licensed to Berend Post berend.post@it-university.nl

cryptography has usually involved the creation and sharing of a secret key for the encryption and decryption of messages. This secret or private key system has the significant flaw that if the key is discovered or intercepted by someone else, messages can easily be decrypted. For this reason, public key cryptography and the public key infrastructure is the preferred approach on the Internet. (The private key system is sometimes known as symmetric cryptography and the public key system as asymmetric cryptography.)

A public key infrastructure consists of:

A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key

A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requester

A Subscriber is the end user who wish to get digital certificate from certificate authority.

The following were incorrect answers:

The Certificate authority role is to issue digital certificates to end users - This is a valid statement as the job of a certificate authority is to issue a digital certificate to end user.

The Registration authority (RA) acts as a verifier for Certificate Authority (CA) - This is a valid statement as registration authority acts as a verifier for certificate authority

Root certificate authority's certificate is always self-signed - This is a valid statement as the root certificate authority's certificate is always self-signed.

The following reference(s) were/was used to create this question:

http://searchsecurity.techtarget.com/definition/PKI

Licensed to Berend Post berend.post@it-university.nl

Question 2702

The quality of the metadata produced from a data warehouse is _____ in the warehouse's design.

- ☐ Often hard to determine because the data is derived from a heterogeneous data environment
- ☒ The most important consideration
- ☐ Independent of the quality of the warehoused databases
- ☐ Of secondary importance to data warehouse content

Explanation:

Explanation:

The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

Question 2703

To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

- ☐ project management tools.
- ☐ an object-oriented architecture.
- ☐ tactical planning.
- ☒ enterprise architecture (EA).

Explanation:

Explanation:

Enterprise architecture (EA) involves documenting the organization's IT assets and processes in a structured manner to facilitate understanding, management and planning for IT investments. It involves both a current state and a representation of an optimized future state. In attempting to complete an EA, organizations can address the problem either from a technology perspective or a business process perspective. Project management does not consider IT investment aspects; it is a tool to aid in delivering projects. Object-oriented architecture is a software development methodology and does not assist in planning for IT investment, while tactical planning is relevant only after high-level IT investment decisions have been made.

Question 2704

Which of the following is the MOST effective approach for integrating security into application development?

- ☐ Including security in user acceptance testing sign-off
- ☐ Performing vulnerability scans
- ☐ Developing security models in parallel
- ☒ Defining security requirements

Licensed to Berend Post berend.post@it-university.nl

Question 2705

An IS auditor has been asked to participate in the creation of an organization's formal business continuity program. Which of the following would impair auditor independence?

- ☒ Developing disaster recovery test scenarios
- ☐ Determining system criticality
- ☐ Facilitating the business impact analysis (BIA)
- ☐ Participating on the business continuity committee

Question 2706

Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

Question 2707

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- ☐ A sufficient quantity of data for each test case
- ☒ Data representing conditions that are expected in actual processing
- ☐ Completing the test on schedule
- ☐ A random sample of actual data

Explanation:

Explanation: Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity. It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

Licensed to Berend Post berend.post@it-university.nl

Question 2708

An organization is replacing its financial processing system. To help ensure that transactions in the new system are processed accurately, which of the following is MOST appropriate?

- ☐ Compare year-to-date balances between the systems.
- ☒ Reconcile results of parallel processing.
- ☐ Document and test internal controls over the conversion.
- ☐ Review data file conversion procedures.

Question 2709

Which of the following protocol uses serial interface for communication between two computers in WAN technology?

- ☒ Point-to-point protocol
- ☐ X.25
- ☐ Frame Relay
- ☐ ISDN

Explanation:

PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer using a MODEM connected by phone line to a server.

For your exam you should know below information about WAN Technologies:

Point-to-point protocol

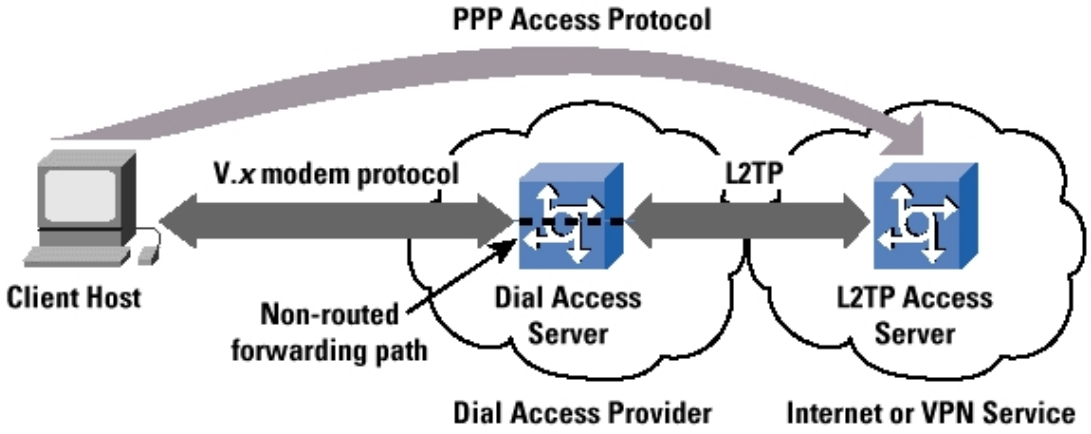
PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet protocol (IP) (and is designed to handle others). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of High Speed Data Link Control (HDLC) for packet encapsulation.

PPP is usually preferred over the earlier de facto standard Serial Line Internet Protocol (SLIP) because it can handle synchronous as well as asynchronous communication. PPP can share a line with other users and it has error detection that SLIP lacks. Where a choice is possible, PPP is preferred.

Licensed to Berend Post berend.post@it-university.nl

Point-to-point protocol



X.25

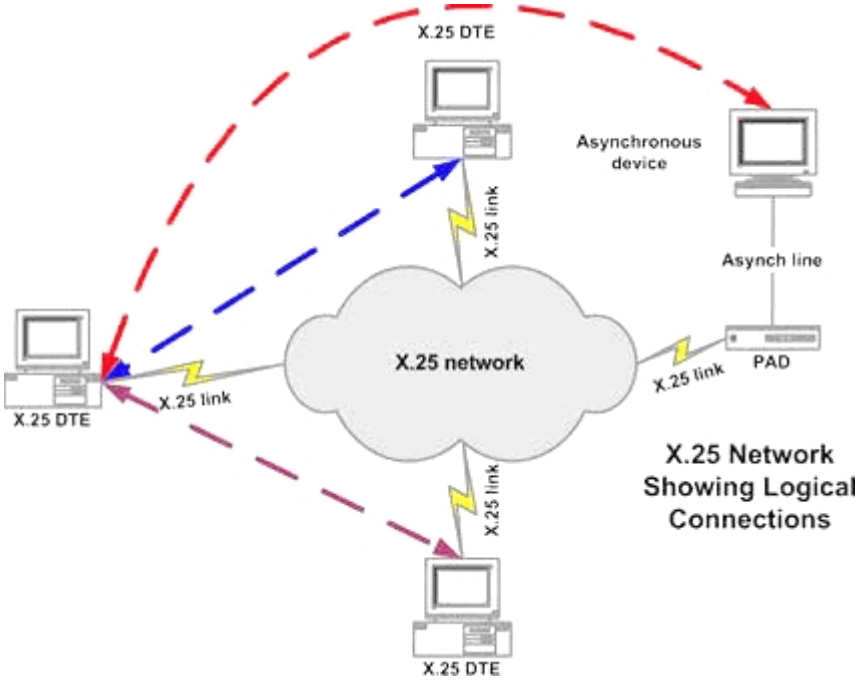
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Subscribers are charged based on amount of bandwidth they use. Data are divided into 128 bytes and encapsulated in High Level Data Link Control (HDLC).

X.25 works at network and data link layer of an OSI model.

Licensed to Berend Post berend.post@it-university.nl



X.25

Frame Relay

Works on a packet switching

Operates at data link layer of an OSI model

Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

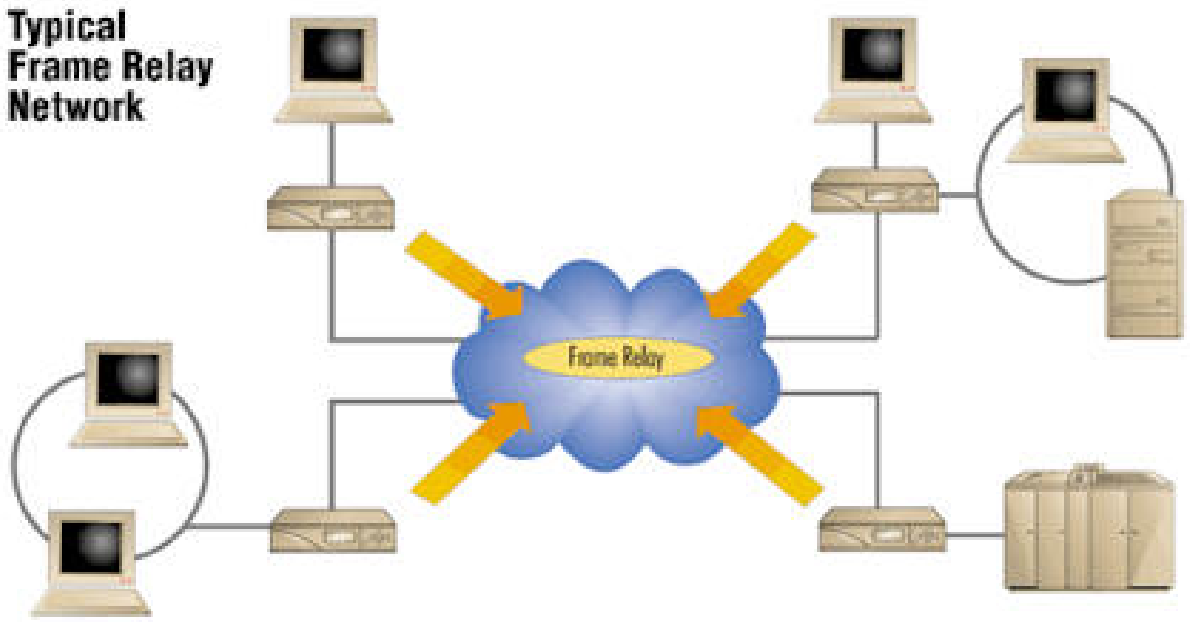
Two main types of equipment's are used in Frame Relay

1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides a connectivity between company's own network and the frame relay's network.

2. Data Circuit Terminal Equipment (DCE) - Service provider device that does the actual data transmission and switching in the frame relay cloud.

The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

Licensed to Berend Post berend.post@it-university.nl



Frame Relay

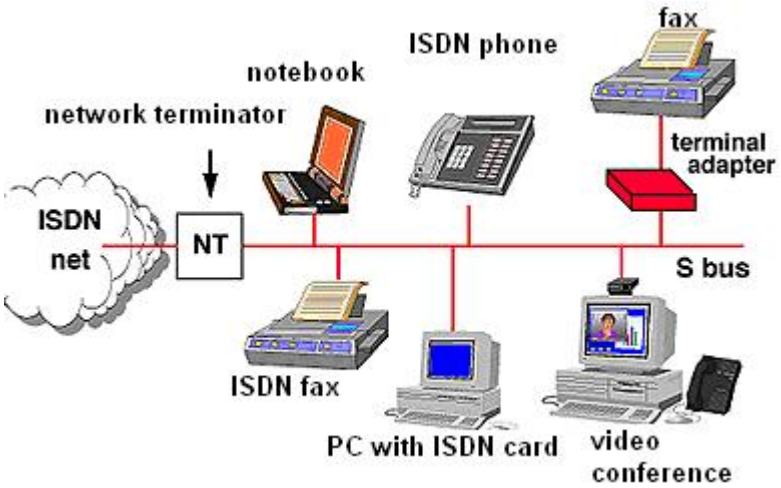
Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.

ISDN



Licensed to Berend Post berend.post@it-university.nl

Asynchronous Transfer Mode (ATM)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel

Data are segmented into fixed size cell of 53 bytes

Some companies have replaced FDDI back-end with ATM

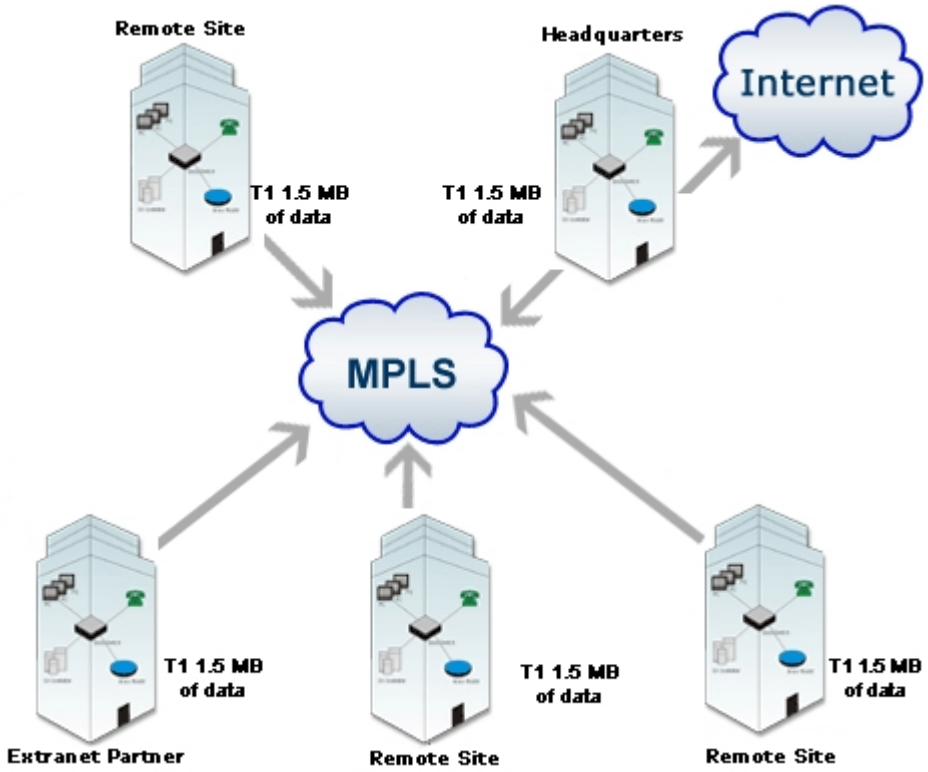
Asynchronous Transfer Mode

Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to. MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

MPLS

Licensed to Berend Post berend.post@it-university.nl



The following answers are incorrect:

X.25 - X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

Frame Relay - The Frame relay cloud is the collection of DCE that provides that provides switching and data communication functionality. Frame relay is any to any service.

ISDN -Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission. Same copper telephone wire is used. Provide digital point-to-point circuit switching medium.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 266

Licensed to Berend Post berend.post@it-university.nl

Question 2710

Parity bits are a control used to validate:

- ☐ Data authentication
- ☒ Data completeness
- ☐ Data source
- ☐ Data accuracy

Explanation:

Explanation:

Parity bits are a control used to validate data completeness.

Question 2711

Which of the following is a distinguishing feature at the highest level of a maturity model?

- ☐ There are formal standards and procedures.
- ☐ Projects are controlled with management supervision.
- ☒ A continuous improvement process is applied.
- ☐ Processes are monitored continuously.

Question 2712

Which of the following can be thought of as the simplest and almost cheapest type of firewall?

- ☐ stateful firewall
- ☐ hardware firewall
- ☐ PIX firewall
- ☒ packet filter
- ☐ None of the choices.

Explanation:

Explanation:

The simplest and almost cheapest type of firewall is a packet filter that stops messages with inappropriate network addresses. It usually consists of a screening router and a set of rules that accept or reject a message based on information in the message header.

Licensed to Berend Post berend.post@it-university.nl

Question 2713

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them. zombie computers are being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☒ DDoS
- ☐ ATP
- ☐ Social Engineering
- ☐ None of the choices.

Explanation:

Explanation: "Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (""zombie computers"") are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion."

Question 2714

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

- ☒ translates information security policies and standards into business requirements.
- ☐ articulates management's intent and information security directives in clear language.
- ☐ relates the investment to the organization's strategic plan.
- ☐ realigns information security objectives to organizational strategy.

Question 2715

An organization is running servers with critical business applications that are in an area subject to frequent but brief power outages. Knowledge of which of the following would allow the organization's management to monitor the ongoing adequacy of the uninterrupted power supply (UPS)?

- ☐ Duration and interval of the power outages
- ☒ Business impact of server downtime
- ☐ Number of servers supported by the UPS
- ☐ Mean time to recover servers after failure

Licensed to Berend Post berend.post@it-university.nl

Question 2716

Which of the following level in CMMI model focuses on process definition and process deployment?

- ☐ Level 4
- ☐ Level 5
- ☒ Level 3
- ☐ Level 2

Explanation:

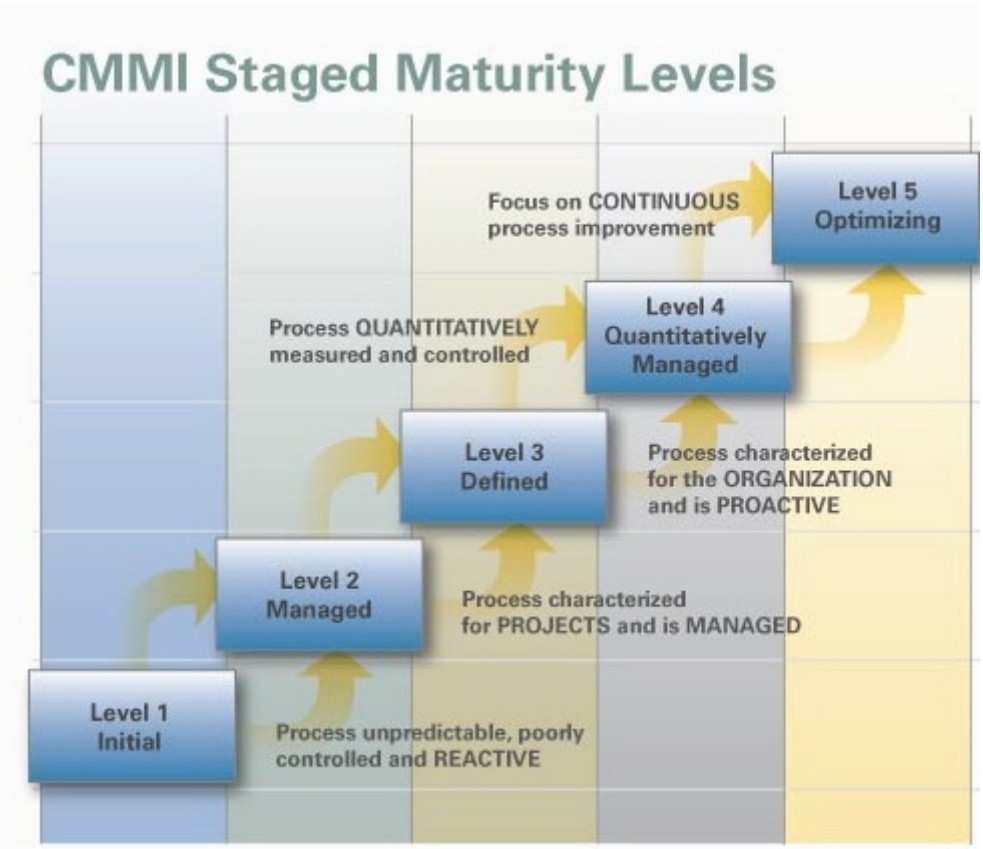
Level 3 is the defined step and focus on process definition and process deployment.

For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.

CMMI Levels



Licensed to Berend Post berend.post@it-university.nl

A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organizations' software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".[citation needed]

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.

Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions).

Licensed to Berend Post berend.post@it-university.nl

Managed - the process is quantitatively managed in accordance with agreed-upon metrics.

Optimizing - process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

Licensed to Berend Post berend.post@it-university.nl

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

The following were incorrect answers:

Level 4 – Focus on process management and process control

Level 5 – Process innovation and continuous optimization.

Level 2 – Performance management and work product management.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 188

Question 2717

Which of the following would be the BEST access control procedure?

- ☒ The data owner formally authorizes access and an administrator implements the user authorization tables.
- ☐ Authorized staff implements the user authorization tables and the data owner sanctions them.
- ☐ The data owner and an IS manager jointly create and update the user authorization tables.
- ☐ The data owner creates and updates the user authorization tables.

Explanation:

Explanation:

The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

Licensed to Berend Post berend.post@it-university.nl

Question 2718

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- ☒ Modems convert analog transmissions to digital, and digital transmission to analog.
- ☐ Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
- ☐ Modems convert digital transmissions to analog, and analog transmissions to digital.
- ☐ Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Explanation:

Explanation:

Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

Question 2719

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- ☒ has a decreased risk of leakage.
- ☐ is more effective at suppressing flames.
- ☐ allows more time to abort release of the suppressant.
- ☐ disperses dry chemical suppressants exclusively.

Question 2720

Which of the following provides the GREATEST assurance that an organization allocates appropriate resources to respond to information security events?

- ☐ Incident classification procedures
- ☐ Threat analysis and intelligence reports
- ☒ An approved IT staffing plan
- ☐ Information security policies and standards.

Question 2721

Reorganization of databases is undertaken PRIMARILY to:

- ☐ reduce backout and recovery times.
- ☐ eliminate duplicates and perform data backup.
- ☐ reduce simultaneous update time and index validation.
- ☒ improve data access and retrieval times.

Licensed to Berend Post berend.post@it-university.nl

Question 2722

Which of the following would a digital signature MOST likely prevent?

- ☒ Corruption
- ☐ Unauthorized change
- ☐ Repudiation
- ☐ Disclosure

Explanation:

Explanation:

The main reason of using digital signature is to ensure message integrity.it also helps to ensure authenticity and non-repudiation of the message. A digital signature can never ensure the confidentiality of data

Question 2723

Which of the following would be the MOST appropriate reason for an organization to purchase fault-tolerant hardware?

- ☐ Reducing hardware maintenance costs.
- ☐ Improving system performance.
- ☒ Minimizing business loss.
- ☐ Compensating for the lack of contingency planning

Question 2724

To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

- ☐ enterprise data model.
- ☒ IT balanced scorecard (BSC).
- ☐ IT organizational structure.
- ☐ historical financial statements.

Explanation:

Explanation:

The IT balanced scorecard (BSC) is a tool that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. An enterprise data model is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity. Historical financial statements do not provide information about planning and lack sufficient detail to enable one to fully understand management’s activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

Licensed to Berend Post berend.post@it-university.nl

Question 2725

An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the BESTassurance that the third party's contract programmers comply with the organization's security policies?

- ☒ Perform periodic security assessments of the contractors' activities.
- ☐ Conduct periodic vulnerability scans of the application.
- ☐ Include penalties for noncompliance in the contracting agreement.
- ☐ Require annual signed agreements of adherence to security policies.

Question 2726

Which of the following is the PRIMARY reason for an IS auditor to issue an interim audit report?

- ☐ To avoid issuing a final audit report
- ☐ To enable the auditor to complete the engagement in a timely manner
- ☒ To provide feedback to the auditee for timely remediation
- ☐ To provide follow-up opportunity during the audit

Question 2727

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

- ☒ A monitored double-doorway entry system
- ☐ A monitored turnstile entry system
- ☐ A monitored doorway entry system
- ☐ A one-way door that does not allow exit after entry

Explanation:

Explanation:

A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used a deterrent control for the vulnerability of piggybacking.

Question 2728

An organization allows employee use of personal mobile devices for corporate email. Which of the following should be the GREATEST IS audit concern?

- ☐ Email forwarding to private devices requires excessive network bandwidth
- ☒ There is no corporate policy for the acceptable use of private devices
- ☐ There is no adequate tracking of the working time spent out-of-hours
- ☐ The help desk is not able to fully support different kinds of private devices

Licensed to Berend Post berend.post@it-university.nl

Question 2729

A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

- ☐ Key verification
- ☐ One-for-one checking
- ☐ Manual recalculations
- ☒ Functional acknowledgements

Explanation:

Explanation:

Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

Question 2730

An organization is planning to replace its wired networks with wireless networks. Which of the following would BEST secure the wireless network from unauthorized access?

- ☐ Implement Wired Equivalent Privacy (WEP)
- ☐ Permit access to only authorized Media Access Control (MAC) addresses
- ☐ Disable open broadcast of service set identifiers (SSID)
- ☒ Implement Wi-Fi Protected Access (WPA) 2

Explanation:

Explanation:

Wi-Fi Protected Access (WPA) 2 implements most of the requirements of the IEEE 802.11i standard. The Advanced Encryption Standard (AESJ used in WPA2 provides better security. Also, WPA2 supports both the Extensible Authentication Protocol and the preshared secret key authentication model. Implementing Wired Equivalent Privacy (WEP) is incorrect since it can be cracked within minutes. WEP uses a static key which has to be communicated to all authorized users, thus management is difficult. Also, there is a greater vulnerability if the static key is not changed at regular intervals. The practice of allowing access based on Media Access Control (MAC) is not a solution since MAC addresses can be spoofed by attackers to gain access to the network. Disabling open broadcast of service set identifiers (SSID) is not the correct answer as they cannot handle access control.

Question 2731

An IS auditor would MOST likely recommend that IT management use a balanced scorecard to:

- ☐ ensure that IT staff meet performance requirements.
- ☐ train and educate IT staff.
- ☐ indicate whether the organization meets quality standards.
- ☒ assess IT functions and processes.

Licensed to Berend Post berend.post@it-university.nl

Question 2732

A large organization is considering a policy that would allow employees to bring their own smartphones into the organizational environment. The MOST important concern to the information security manager should be the:

- ☒ lack of a device management solution.
- ☐ decrease in end user productivity.
- ☐ impact on network capacity.
- ☐ higher costs in supporting end users.

Question 2733

Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

- ☒ Legal and compliance requirements
- ☐ Customer agreements
- ☐ Organizational policies and procedures
- ☐ Data classification

Question 2734

Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

- ☐ Backup time would steadily increase
- ☐ Backup operational cost would significantly increase
- ☐ Storage operational cost would significantly increase
- ☒ Server recovery work may not meet the recovery time objective (RTO)

Explanation:

Explanation:

In case of a crash, recovering a server with an extensive amount of data could require a significant amount of time. If the recovery cannot meet the recovery time objective (RTO), there will be a discrepancy in IT strategies. It's important to ensure that server restoration can meet the RTO. Incremental backup would only take the backup of the daily differential, thus a steady increase in backup time is not always true. The backup and storage costs issues are not as significant as not meeting the RTO.

Licensed to Berend Post berend.post@it-university.nl

Question 2735

The phases and deliverables of a system development life cycle (SDLC) project should be determined:

- ☒ during the initial planning stages of the project.
- ☐ after early planning has been completed, but before work has begun.
- ☐ throughout the work stages, based on risks and exposures.
- ☐ only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

Explanation:

Explanation:

It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

Question 2736

A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:

- ☐ date and time stamp of the message.
- ☐ identity of the originating computer.
- ☐ confidentiality of the message's content.
- ☒ authenticity of the sender.

Explanation:

Explanation:

The signature on the digest can be used to authenticate the sender. It does not provide assurance of the date and time stamp or the identity of the originating computer. Digitally signing an e-mail message does not prevent access to its content and, therefore, does not assure confidentiality.

Question 2737

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following?

- ☐ IT strategic plan
- ☒ Business continuity plan
- ☐ Business impact analysis
- ☐ Incident response plan

Explanation:

Explanation:

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

Licensed to Berend Post berend.post@it-university.nl

Question 2738

Which of the following is MOST important when selecting an information security metric?

- ☒ Defining the metric in quantitative terms
- ☐ Aligning the metric to the IT strategy
- ☐ Defining the metric in qualitative terms
- ☐ Ensuring the metric is repeatable

Question 2739

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

- ☒ A dry-pipe sprinkler system
- ☐ A deluge sprinkler system
- ☐ A wet-pipe system
- ☐ A halon sprinkler system

Explanation:

Explanation:

A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

Question 2740

Which of the following provides the MOST comprehensive description of IT's role in an organization?

- ☐ IT organizational chart
- ☐ IT project portfolio
- ☒ IT charter
- ☐ IT job description

Question 2741

An external penetration test identified a serious security vulnerability in a critical business application. Before reporting the vulnerability to senior management, the information security manager's BEST course of action should be to:

- ☒ determine the potential impact with the business owner
- ☐ initiate the incident response process
- ☐ block access to the vulnerable business application
- ☐ report the vulnerability to IT for remediation

Licensed to Berend Post berend.post@it-university.nl

Question 2742

Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

- ☐ Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
- ☐ Secure Sockets Layer (SSL) mode
- ☒ Tunnel mode with AH plus ESP
- ☐ Triple-DES encryption mode

Explanation:

Explanation:Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL mode provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality.

Question 2743

A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

- ☐ Introduce a secondary authentication method such as card swipe
- ☒ Apply role-based permissions within the application system
- ☐ Have users input the ID and password for each database transaction
- ☐ Set an expiration period for the database password embedded in the program

Explanation:

Explanation:

When a single ID and password are embedded in a program, the best compensating control would be a sound access control over the application layer and procedures to ensure access to data is granted based on a user's role. The issue is user permissions, not authentication, therefore adding a stronger authentication does not improve the situation. Having a user input the ID and password for access would provide a better control because a database log would identify the initiator of the activity. However, this may not be efficient because each transaction would require a separate authentication process. It is a good practice to set an expiration date for a password. However, this might not be practical for an ID automatically logged in from the program. Often, this type of password is set not to expire.

Licensed to Berend Post berend.post@it-university.nl

Question 2744

During an IS audit, it is discovered that security configurations differ across the organization's virtual server farm. Which of the following is the IS auditor's BEST recommendation for improving the control environment?

- ☐ Conduct an independent review of each server's security configuration
- ☒ Implement a security configuration baseline for virtual servers
- ☐ Implement security monitoring controls for high-risk virtual servers
- ☐ Conduct a standard patch management review across the virtual server farm

Question 2745

Which of the following should be an information security manager's PRIMARY role when an organization initiates a data classification process?

- ☐ Assign the asset classification level.
- ☒ Define the classification structure to be implemented.
- ☐ Verify that assets have been appropriately classified.
- ☐ Apply security in accordance with specific classification.

Question 2746

If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

- ☒ To advise senior management.
- ☐ To reassign job functions to eliminate potential fraud.
- ☐ To implement compensator controls.
- ☐ Segregation of duties is an administrative control not considered by an IS auditor.

Explanation:

Explanation:

An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

Licensed to Berend Post berend.post@it-university.nl

Question 2747

Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

- ☐ database integrity checks.
- ☐ validation checks.
- ☐ input controls.
- ☒ database commits and rollbacks.

Explanation:

Explanation:

Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

Question 2748

Which of the following is the most important benefit of control self-assessment (CSA)?

- ☐ CSA is a policy/rule driven
- ☒ In CSA approach, risk is identified sooner
- ☐ CSA requires limited employee participations
- ☐ In CSA, resources are being used in an effective manner.

Explanation:

Explanation:

Control self-assessment is an assessment of controls made by staff and management within the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal controls of the organization are reliable. The CSA approach requires extensive employee participations and training. This will help to employee understand more about business risks. This will insure the detection of risk in timely manner.

For your exam you should know the information below about control self-assessment:

Benefits of CSA

Early detection of risk

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives

Licensed to Berend Post berend.post@it-university.nl

Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

Highly motivated employees

Improved audit training process

Reduction in control cost

Assurance provided to stakeholders and customers

Traditional and CSA attributes

Traditional Historical CSA

Assign duties/supervises staff Empowered/accountable employees

Policy/rule driven Continuous improvement/learning curve

Limited employee participation Extensive employee participation and training

Narrow stakeholders focus Broad stakeholders focus

Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are incorrectly describes about CSA.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 61, 62 and 63

Question 2749

Which of the following BEST provides continuous availability of network bandwidth for critical application services?

- ☐ Configuration management
- ☐ Cloud computing
- ☐ Problem management
- ☒ Quality of service (QoS)

Licensed to Berend Post berend.post@it-university.nl

Question 2750

Which of the following is the PRIMARY benefit of using an integrated audit approach?

- ☐ Higher acceptance of the findings from the audited business areas
- ☐ The avoidance of duplicated work and redundant recommendations
- ☐ Enhanced allocation of resources and reduced audit costs
- ☒ A holistic perspective of overall risk and a better understanding of controls

Question 2751

Which of the following terms refers to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders?

- ☒ ILD&P
- ☐ ICT&P
- ☐ ILP&C
- ☐ ILR&D
- ☐ None of the choices.

Explanation:

Explanation:

Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

Question 2752

When developing a disaster recovery plan, the criteria for determining the acceptable downtime should be the:

- ☐ annualized loss expectancy (ALE).
- ☐ service delivery objective.
- ☐ quantity of orphan data.
- ☒ maximum tolerable outage.

Explanation:

Explanation:

The recovery time objective is determined based on the acceptable downtime in case of a disruption of operations, it indicates the maximum tolerable outage that an organization considers to be acceptable before a system or process must resume following a disaster. Choice A is incorrect, because the acceptable downtime would not be determined by the annualized loss expectancy (ALE). Choices B and C are relevant to business continuity, but they are not determined by acceptable downtime.

Licensed to Berend Post berend.post@it-university.nl

Question 2753

The MOST significant reason for using key performance indicators (KPIs) to track the progress of IT projects against initial targets is that they:

- ☐ influence management decisions to outsource IT projects
- ☐ identify which projects may require additional funding
- ☐ provide timely indication of when corrective actions need to be taken
- ☒ identify instances where increased stakeholder engagement is required

Question 2754

An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

- ☐ Administrative security can be provided for the client.
- ☒ System administration can be better managed.
- ☐ The security of the desktop PC is enhanced.
- ☐ Desktop application software will never have to be upgraded.

Question 2755

Run-to-run totals can verify data through which stage(s) of application processing?

- ☐ Initial
- ☒ Various
- ☐ Final
- ☐ Output

Explanation:

Explanation:

Run-to-run totals can verify data through various stages of application processing.

Question 2756

Which of the following would prevent unauthorized changes to information stored in a server's log?

- ☐ Write-protecting the directory containing the system log
- ☐ Writing a duplicate log to another server
- ☐ Daily printing of the system log
- ☒ Storing the system log in write-once media

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Storing the system log in write-once media ensures the log cannot be modified. Write- protecting the system log does not prevent deletion or modification, since the superuser or users that have special permission can override the write protection. Writing a duplicate log to another server or daily printing of the system log cannot prevent unauthorized changes.

Question 2757

In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

- ☒ Testing whether inappropriate personnel can change application parameters
- ☐ Tracing purchase orders to a computer listing
- ☐ Comparing receiving reports to purchase order details
- ☐ Reviewing the application documentation

Explanation:

Explanation:

To determine purchase order validity, testing access controls will provide the best evidence. Choices B and C are based on after-the-fact approaches, while choice D does not serve the purpose because what is in the system documentation may not be the same as what is happening.

Question 2758

Passwords should be:

- ☒ assigned by the security administrator for first time logon.
- ☐ changed every 30 days at the discretion of the user.
- ☐ reused often to ensure the user does not forget the password.
- ☐ displayed on the screen so that the user can ensure that it has been entered properly.

Explanation:

Explanation:

Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

Licensed to Berend Post berend.post@it-university.nl

Question 2759

A certificate authority (CA) can delegate the processes of:

- ☐ revocation and suspension of a subscriber's certificate.
- ☐ generation and distribution of the CA public key.
- ☒ establishing a link between the requesting entity and its public key.
- ☐ issuing and distributing subscriber certificates.,

Explanation:

Explanation:

Establishing a link between the requesting entity and its public key is a function of a registration authority. This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform.

Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

Question 2760

Which of the following is the GREATEST risk of single sign-on?

- ☐ Password carelessness by one user may render the entire infrastructure vulnerable
- ☒ Integration of single sign-on with the rest of the infrastructure is complicated
- ☐ It is a single point of failure for an enterprise access control process
- ☐ One administrator maintains the single sign-on solutions without segregation of duty

Question 2761

Which of the following control helps to identify an incident’s activities and potentially an intruder?

- ☐ Deterrent
- ☐ Preventive
- ☒ Detective
- ☐ Compensating

Explanation:

Explanation:

Detective control helps identify an incident’s activities and potentially an intruder

For your exam you should know below information about different security controls

Deterrent Controls

Licensed to Berend Post berend.post@it-university.nl

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

Licensed to Berend Post berend.post@it-university.nl

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Licensed to Berend Post berend.post@it-university.nl

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

Preventive - Preventive controls are intended to avoid an incident from occurring

Compensating - Compensating Controls provide an alternative measure of control

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Licensed to Berend Post berend.post@it-university.nl

Question 2762

The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:

- ☐ maintain compliance with industry best practices.
- ☒ serve as evidence of security awareness training.
- ☐ assign accountability for transactions made with the user's ID.
- ☐ maintain an accurate record of users' access rights.

Question 2763

An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

- ☐ tested every six months.
- ☒ regularly reviewed and updated.
- ☐ approved by the chief executive officer (CEO).
- ☐ communicated to every department head in the organization.

Explanation:

Explanation:

The plan should be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel. Otherwise, it may become out of date and may no longer be effective. The plan must be subjected to regular testing, but the period between tests will again depend on the nature of the organization and the relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. Similarly, although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communications staff.

Question 2764

An IS auditor submitted audit reports and scheduled a follow-up audit engagement with a client. The client has requested to engage the services of the same auditor to develop enhanced controls. What is the GREATEST concern with this request?

- ☐ It would require the approval of the audit manager.
- ☐ It would be beyond the original audit scope.
- ☒ It would a possible conflict of interest.
- ☐ It would require a change to the audit plan.

Licensed to Berend Post berend.post@it-university.nl

Question 2765

During an audit of the organization's data privacy policy, the IS auditor identified that only some IT application databases have encryption in place. What should be the auditor's FIRST action?

- ☐ Assess the resources required to implement encryption to unencrypted databases.
- ☐ Review the most recent database penetration testing results.
- ☒ Determine whether compensating controls are in place.
- ☐ Review a comprehensive list of databases with the information they contain.

Question 2766

An organization is considering allowing users to connect personal devices to the corporate network. Which of the following should be done FIRST?

- ☐ Configure users on the mobile device management solution.
- ☐ Create inventory records of personal devices.
- ☒ Implement an acceptable use policy.
- ☐ Conduct security awareness training.

Question 2767

Which of the following is BEST for providing uninterrupted services?

- ☐ Snapshots
- ☐ Differential backup
- ☐ Televaulting
- ☒ Mirroring

Question 2768

Properly planned risk-based audit programs are often capable of offering which of the following benefits?

- ☒ audit efficiency and effectiveness.
- ☐ audit efficiency only.
- ☐ audit effectiveness only.
- ☐ audit transparency only.
- ☐ audit transparency and effectiveness.
- ☐ None of the choices.

Explanation:

Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

Licensed to Berend Post berend.post@it-university.nl

Question 2769

What is the most common purpose of a virtual private network implementation?

☒ A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.
☐ A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connection.
☐ A virtual private network (VPN) helps to secure access within an enterprise when communicating over a dedicated T1 connection between network segments within the same facility.
☐ A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connection.

Explanation:

Explanation:

A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.

Question 2770

Data edits are implemented before processing and are considered which of the following?

☐ Deterrent integrity controls
☐ Detective integrity controls
☐ Corrective integrity controls
☒ Preventative integrity controls

Explanation:

Explanation:

Data edits are implemented before processing and are considered preventive integrity controls.

Question 2771

Which of the following is the GREATEST risk to the effectiveness of application system controls?

☐ Removal of manual processing steps
☐ inadequate procedure manuals
☒ Collusion between employees
☐ Unresolved regulatory compliance issues

Explanation:

Explanation:

Collusion is an active attack that can be sustained and is difficult to identify since even well-thought-out application controls may be circumvented. The other choices do not impact well-designed application controls.

Licensed to Berend Post berend.post@it-university.nl

Question 2772

As an IS auditor, it is very important to make sure all storage media are well protected. Which of the following is the LEAST important factor for protecting CDs and DVDs?

- ☐ Handle by edges or by the hole in the middle
- ☒ Store in anti-static bag
- ☐ Avoid long term exposure to bright light
- ☐ Store in a hard jewel case, not in soft sleeves

Explanation:

CDs and DVDs are least affected by static current so it is not as important to store them into anti-static bags.

CDs and DVDs Storage protection recommendations:

Handle by edges or by hole in the middle

Be careful not to bend the CD or DVD

Avoid long term exposure to bright light

Store in a hard jewel case, not is soft sleeves

Also, you should know the media storage precautions listed below in preparation for the CISA exam:

USB and portable hard drive

Avoid high temperature, humidity extremes and strong magnetic field

Tape Cartridges

Store Cartridges vertically

Store cartridges in a protective container for transport

Write-protect cartridges immediately

Hard Drive

Store hard drives in anti-static bags, and be sure that person removing them from bag is static free

Licensed to Berend Post berend.post@it-university.nl

If the original box and padding for the hard drive is available, use it for shipping

If the hard drive has been in a cold environment, bring it to room temperature prior to installing and using it

The following reference(s) were/was used to create this question:

Reference used - CISA review manual 2014. Page number 338

Question 2773

Which of the following layer of an OSI model responsible for routing and forwarding of a network packets?

- ☐ Transport Layer
- ☒ Network Layer
- ☐ Data Link Layer
- ☐ Physical Layer

Explanation:

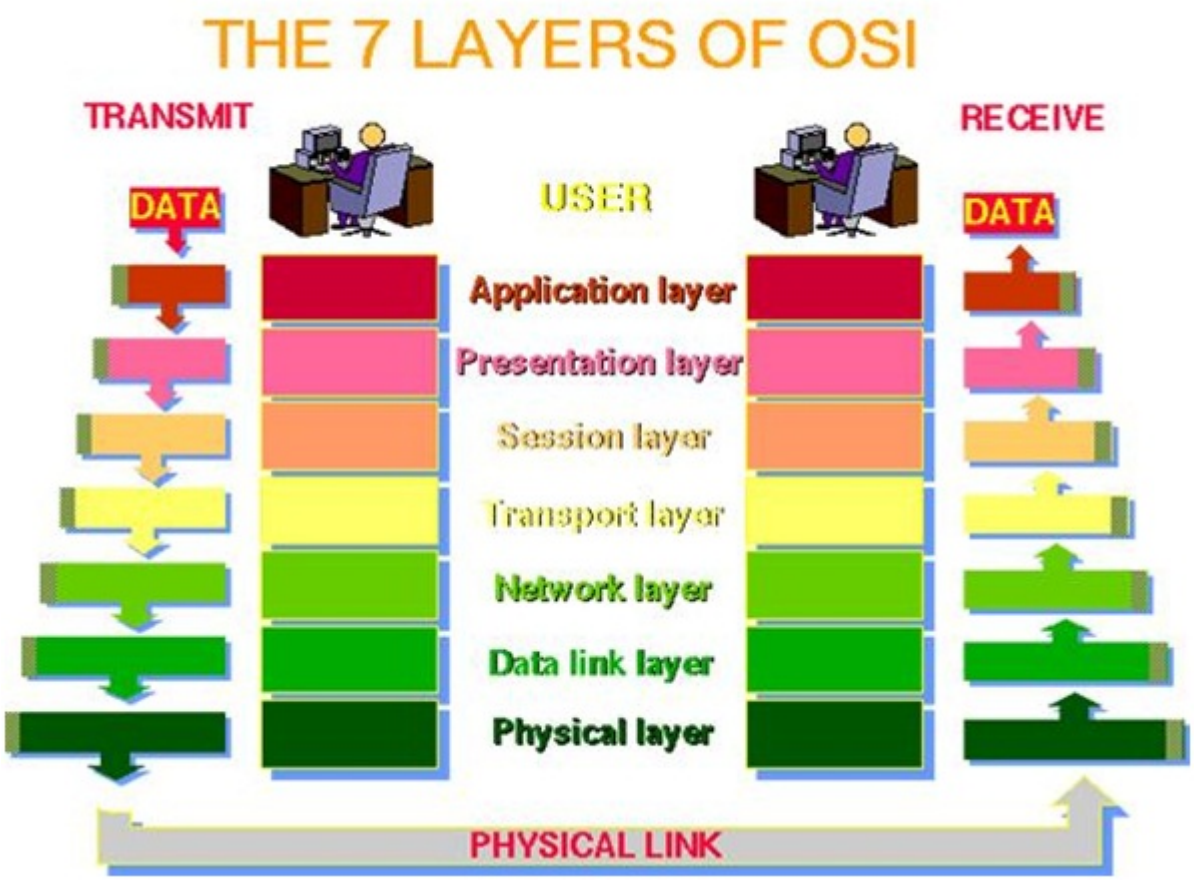
The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.

For CISA exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.OSI Model

Licensed to Berend Post berend.post@it-university.nl



PHYSICAL LAYER

The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

Licensed to Berend Post berend.post@it-university.nl

Link establishment and termination: establishes and terminates the logical link between two nodes.

Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.

Frame sequencing: transmits/receives frames sequentially.

Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.

Frame delimiting: creates and recognizes frame boundaries.

Frame error checking: checks received frames for integrity.

Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.

Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.

Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.

Logical-physical address mapping: translates logical addresses, or names, into physical addresses.

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

Licensed to Berend Post berend.post@it-university.nl

TRANSPORT LAYER

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagram's, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.

Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.

Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.

Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

Licensed to Berend Post berend.post@it-university.nl

The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.

Data compression: reduces the number of bits that need to be transmitted on the network.

Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

Data link layer - The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260

Question 2774

A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

- ☐ validation controls.
- ☐ internal credibility checks.
- ☐ clerical control procedures.
- ☒ automated systems balancing.

Explanation:

Explanation:

Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checks are certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to summarize and compare inputs and outputs, an automated process is less susceptible to error.

Licensed to Berend Post berend.post@it-university.nl

Question 2775

Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

- ☒ the likelihood of a given threat attempting to exploit a vulnerability
- ☐ a function of the cost and effectiveness of controls over a vulnerability
- ☐ the magnitude of the impact should a threat exploit a vulnerability
- ☐ a function of the likelihood and impact, should a threat exploit a vulnerability

Question 2776

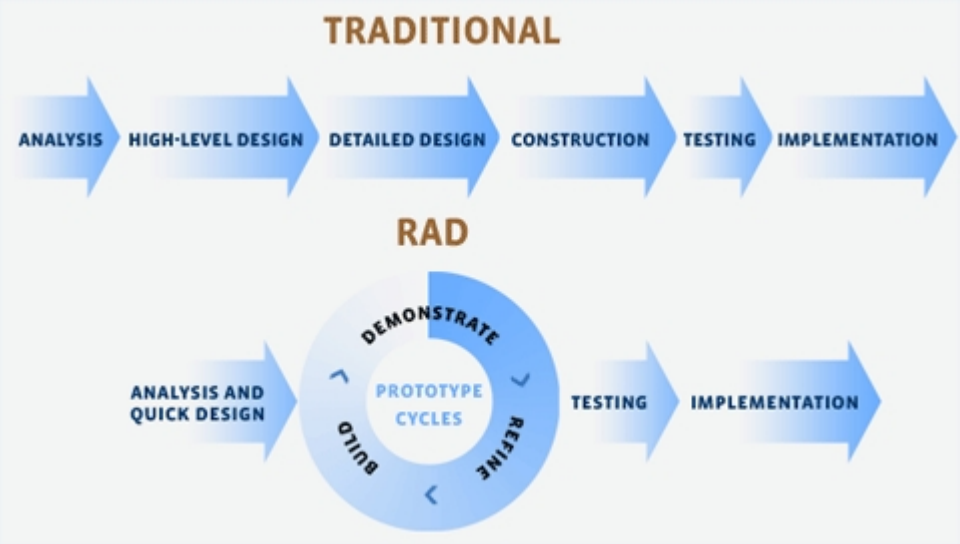
Which of the following software development methodology uses minimal planning and in favor of rapid prototyping?

- ☐ Agile Developments
- ☐ Software prototyping
- ☒ Rapid application development
- ☐ Component based development

Explanation:

Rapid application development (RAD) is a software development methodology that uses minimal planning in favor of rapid prototyping. The "planning" of software developed using RAD is interleaved with writing the software itself. The lack of extensive per-planning generally allows software to be written much faster, and makes it easier to change requirements.

Rapid Application Development



Four phases of RAD

Requirements Planning phase – combines elements of the system planning and systems analysis phases of the Systems Development Life Cycle (SDLC). Users, managers, and IT staff members discuss

Licensed to Berend Post berend.post@it-university.nl

and agree on business needs, project scope, constraints, and system requirements. It ends when the team agrees on the key issues and obtains management authorization to continue.

User design phase – during this phase, users interact with systems analysts and develop models and prototypes that represent all system processes, inputs, and outputs. The RAD groups or subgroups typically use a combination of Joint Application Development (JAD) techniques and CASE tools to translate user needs into working models. User Design is a continuous interactive process that allows users to understand, modify, and eventually approve a working model of the system that meets their needs.

Construction phase – focuses on program and application development task similar to the SDLC. In RAD, however, users continue to participate and can still suggest changes or improvements as actual screens or reports are developed. Its tasks are programming and application development, coding, unit-integration and system testing.

Cutover phase – resembles the final tasks in the SDLC implementation phase, including data conversion, testing, changeover to the new system, and user training. Compared with traditional methods, the entire process is compressed. As a result, the new system is built, delivered, and placed in operation much sooner.

The following were incorrect answers:

Agile Development - Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

Component Based Development - It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

The following reference(s) were/was used to create this question:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 Page number 195

Question 2777

Which of the following would be the MOST effective control to reduce the risk of information leakage through social media?

- ☐ Use of keystroke loggers
- ☐ Periodic review of the data classification policy
- ☐ Limited access to social media sites in the workplace
- ☒ Security awareness training

Question 2778

The success of an IT projects is measured PRIMARILY by the:

- ☐ translation of business vision to function vision
- ☐ implementation of current technology
- ☒ benefit that the business derives from the outcome
- ☐ efficient use of resources

Question 2779

Which of the following should be the PRIMARY reason to establish a social media policy for all employees?

- ☐ To publish acceptable messages to be used by employees when posting
- ☒ To raise awareness and provide guidance about social media risks
- ☐ To restrict access to social media during business hours to maintain productivity
- ☐ To prevent negative public social media postings and comments

Question 2780

Which of the following is the MOST important element for the successful implementation of IT governance?

- ☐ Implementing an IT scorecard
- ☒ Identifying organizational strategies
- ☐ Performing a risk assessment
- ☐ Creating a formal security policy

Explanation:

Explanation:

The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance.

Licensed to Berend Post berend.post@it-university.nl

Without identification of organizational strategies, the remaining choices-even if implemented-would be ineffective.

Question 2781

Which of the following audit is mainly designed to evaluate the internal control structure in a given process or area?

- ☐ Compliance Audit
- ☐ Financial Audit
- ☒ Operational Audit
- ☐ Forensic audit

Explanation:

Explanation:

Operational audit is mainly designed to evaluate the internal control structure in a given process or area. Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

For your exam you should know below information about different types of audit:

What is an audit?

An audit in general terms is a process of evaluating an individual or organization's accounts. This is usually done by an independent auditing body. Thus, audit involves a competent and independent person obtaining evidence and evaluating it objectively with regard to a given entity, which in this case is the subject of audit, in order to establish conformance to a given set of standards. Audit can be on a person, organization, system, enterprise, project or product.

Compliance Audit

A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Licensed to Berend Post berend.post@it-university.nl

What, precisely, is examined in a compliance audit will vary depending upon whether an organization is a public or private company, what kind of data it handles and if it transmits or stores sensitive financial data. For instance, SOX requirements mean that any electronic communication must be backed up and secured with reasonable disaster recovery infrastructure. Health care providers that store or transmit e-health records, like personal health information, are subject to HIPAA requirements. Financial services companies that transmit credit card data are subject to PCI DSS requirements. In each case, the organization must be able to demonstrate compliance by producing an audit trail, often generated by data from event log management software.

Financial Audit

A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Operational Audit

Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives. Operational audit is a more comprehensive form of an Internal audit.

The Institute of Internal Auditor (IIA) defines Operational Audit as a systematic process of evaluating an organization's effectiveness, efficiency and economy of operations under management's control and reporting to appropriate persons the results of the evaluation along with recommendations for improvement.

Objectives

To appraise the effectiveness and efficiency of a division, activity, or operation of the entity in meeting organizational goals.

To understand the responsibilities and risks faced by an organization.

To identify, with management participation, opportunities for improving control.

To provide senior management of the organization with a detailed understanding of the Operations.

Licensed to Berend Post berend.post@it-university.nl

Integrated Audits

An integrated audit combines financial and operational audit steps. An integrated audit is also performed to assess overall objectives within an organization, related to financial information and asset, safeguarding, efficiency and or internal auditors and would include compliance test of internal controls and substantive audit step.

IS Audit

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

The primary functions of an IT audit are to evaluate the systems that are in place to guard an organization's information. Specifically, information technology audits are used to evaluate the organization's ability to protect its information assets and to properly dispense information to authorized parties. The IT audit aims to evaluate the following:

Will the organization's computer systems be available for the business at all times when required? (known as availability) Will the information in the systems be disclosed only to authorized users? (known as security and confidentiality) Will the information provided by the system always be accurate, reliable, and timely? (measures the integrity) In this way, the audit hopes to assess the risk to the company's valuable asset (its information) and establish methods of minimizing those risks.

Forensic Audit

Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Licensed to Berend Post berend.post@it-university.nl

Compliance Audit - A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Financial Audit- A financial audit, or more accurately, an audit of financial statements, is the verification of the financial statements of a legal entity, with a view to express an audit opinion. The audit opinion is intended to provide reasonable assurance, but not absolute assurance, that the financial statements are presented fairly, in all material respects, and/or give a true and fair view in accordance with the financial reporting framework. The purpose of an audit is to provide an objective independent examination of the financial statements, which increases the value and credibility of the financial statements produced by management, thus increase user confidence in the financial statement, reduce investor risk and consequently reduce the cost of capital of the preparer of the financial statements.

Forensic Audit - Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 44

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

Question 2782

Which of the following groups is MOST likely responsible for the implementation of IT projects?

- ☒ IT steering committee
- ☐ IT compliance committee
- ☐ IT strategy committee
- ☐ IT governance committee

Licensed to Berend Post berend.post@it-university.nl

Question 2783

An IS auditor learns a server administration team regularly applies workarounds to address repeated failures of critical data processing services. Which of the following would BEST enable the organization to resolve this issue?

- ☐ Service level management
- ☐ Change management
- ☒ Problem management
- ☐ Incident management

Question 2784

Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

- ☐ Filters
- ☒ Switches
- ☐ Routers
- ☐ Firewalls

Explanation:

Explanation:

Switches are at the lowest level of network security and transmit a packet to the device to which it is addressed. This reduces the ability of one device to capture the packets that are meant for another device. Filters allow for some basic isolation of network traffic based on the destination addresses. Routers allow packets to be given or denied access based on the addresses of the sender and receiver and the type of packet. Firewalls are a collection of computer and network equipment used to allow communications to flow out of the organization and restrict communications flowing into the organization.

Question 2785

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

- ☐ Halon gas
- ☐ Deluge sprinklers
- ☒ Dry-pipe sprinklers
- ☐ Wet-pipe sprinklers

Explanation:

Explanation:

Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

Licensed to Berend Post berend.post@it-university.nl

Question 2786

Which of the following can provide assurance that an IT project has delivered its planned benefits?

- ☐ User acceptance testing (UAT)
- ☐ Steering committee approval
- ☒ Post-implementation review
- ☐ Quality assurance evaluation

Question 2787

Due to the cost restrains, a company defers the replacement of hardware supporting core application. Which of the following represents the GREATEST risk?

- ☐ Maintenance costs may rise.
- ☐ Future upgrades may not be possible.
- ☒ Systems availability may suffer.
- ☐ Eventual replacement may be more expensive.

Question 2788

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

- ☐ wormnets
- ☐ trojannets
- ☐ spynets
- ☒ botnets
- ☐ rootnets
- ☐ backdoor

Explanation:

Explanation:

In order to coordinate the activity of many infected computers, attackers are used coordinating systems known as botnets. In a botnet, the malware or mailbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

Question 2789

A check digit is an effective edit check to:

- ☐ Detect data-transcription errors
- ☒ Detect data-transposition and transcription errors
- ☐ Detect data-transposition, transcription, and substitution errors
- ☐ Detect data-transposition errors

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A check digit is an effective edit check to detect data-transposition and transcription errors.

Question 2790

What is the recommended minimum length of a good password?

- ☐ 6 characters
- ☒ 8 characters
- ☐ 12 characters
- ☐ 18 characters
- ☐ 22 characters
- ☐ None of the choices.

Explanation:

Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

Question 2791

When installing an intrusion detection system (IDS), which of the following is MOST important?

- ☒ Properly locating it in the network architecture
- ☐ Preventing denial-of-service (DoS) attacks
- ☐ Identifying messages that need to be quarantined
- ☐ Minimizing the rejection errors

Explanation:

Explanation:

Proper location of an intrusion detection system (IDS) in the network is the most important decision during installation. A poorly located IDS could leave key areas of the network unprotected. Choices B, C and D are concerns during the configuration of an IDS, but if the IDS is not placed correctly, none of them would be adequately addressed.

Licensed to Berend Post berend.post@it-university.nl