vce trainer

Reference Solution for isaca.pass4sureexam.cisa.v2020-03-23.by.mohammed.1103q.vce

CISA

CISA

Score:	800/1000
Version:	1
Time Limit:	120 Minutes

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

Exam A (1103 questions)

Question 1

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 2

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 3

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:

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

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 covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

Question 4

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 5

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

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

Question 6

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.

Question 7

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

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

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.

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:

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

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.

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

CISA review manual 2014 Page number 187

Question 8

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.

Question 9

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:

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

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 10

A database is denormalized in order to:

- ☐ prevent loss of data.
- ☒ increase processing efficiency.
- ☐ ensure data integrity.
- ☐ save storage space.

Question 11

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 12

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.

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

Question 13

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 14

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 15

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:

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

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 16

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.

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.

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

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.

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:

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

CISA review manual 2014 Page number 367 and 368

Question 17

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.

Question 18

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 19

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.

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

Question 20

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 21

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.

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:

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 22

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.

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

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

Question 23

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 24

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

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

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 25

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 26

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

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

Question 27

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:

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.

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

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 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.

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

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

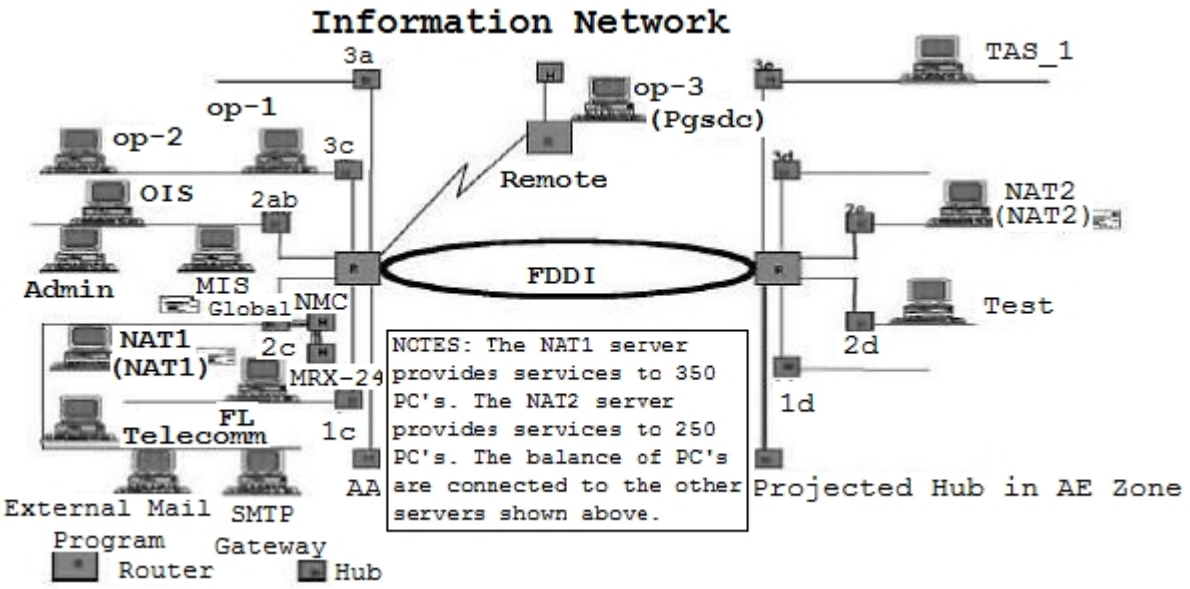
SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities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

Question 28

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:

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

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.

Question 29

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 30

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 31

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

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

Question 32

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 33

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.

Question 34

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

Question 35

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

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

Question 36

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:

Disaster recovery planning (DRP) is the technological aspect of business continuity planning. Business resumption planning addresses the operational part of business continuity planning.

Question 37

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 38

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.

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

Question 39

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 40

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 41

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 42

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:

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

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:

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:

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

CISA review manual 2014 page number 52 and 53

http://www.businessdictionary.com/definition/compliance-test.html

Question 43

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."

Question 44

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 45

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:

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

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 46

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 47

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 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,

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

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 48

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 49

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:

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

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:

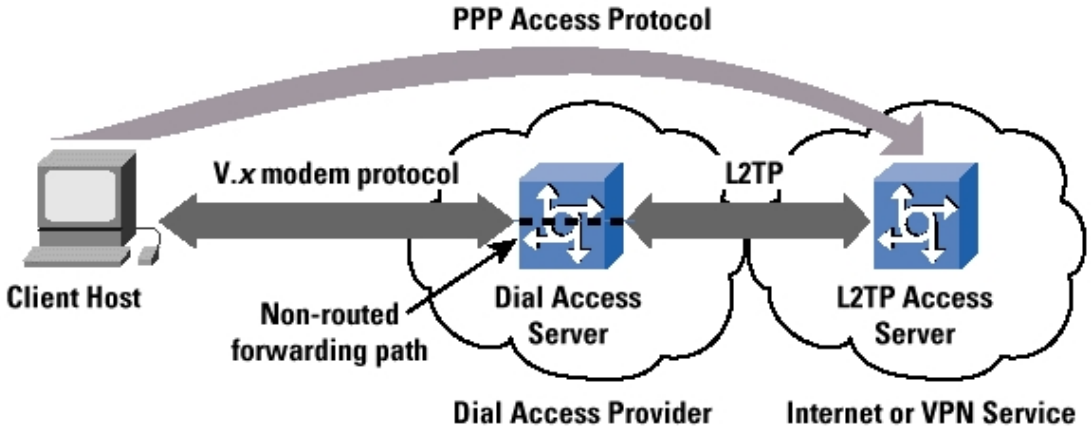
Point-to-point protocol

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.

Point-to-point protocol



X.25

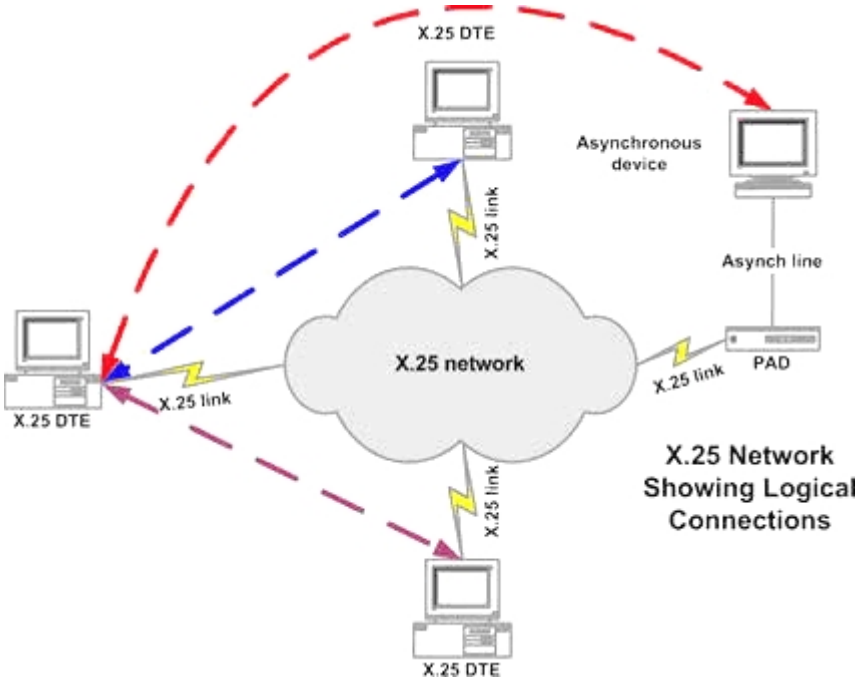
Licensed to Berend Post berend.post@it-university.nl

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.

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

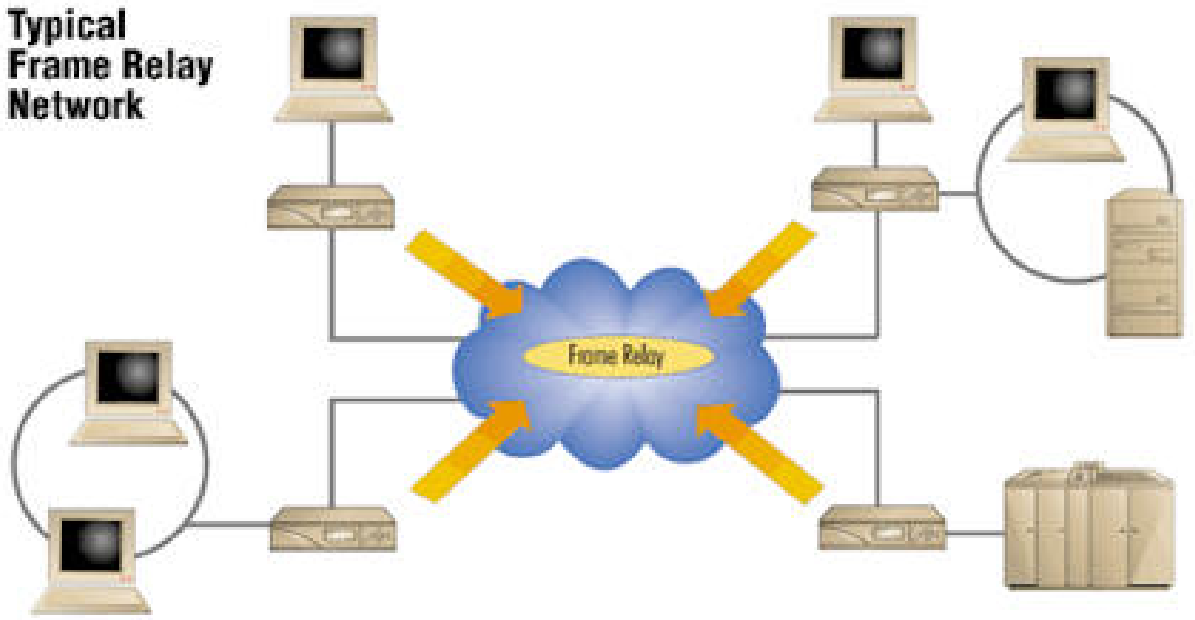
Two main types of equipment’s are used in Frame Relay

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.

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

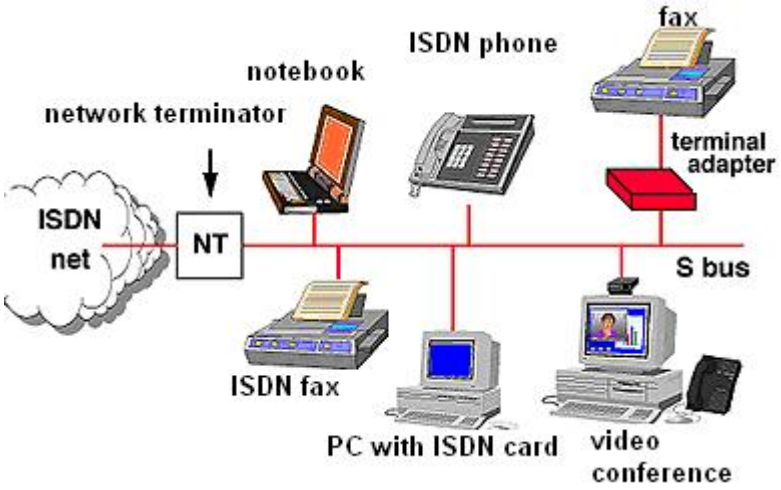
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

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

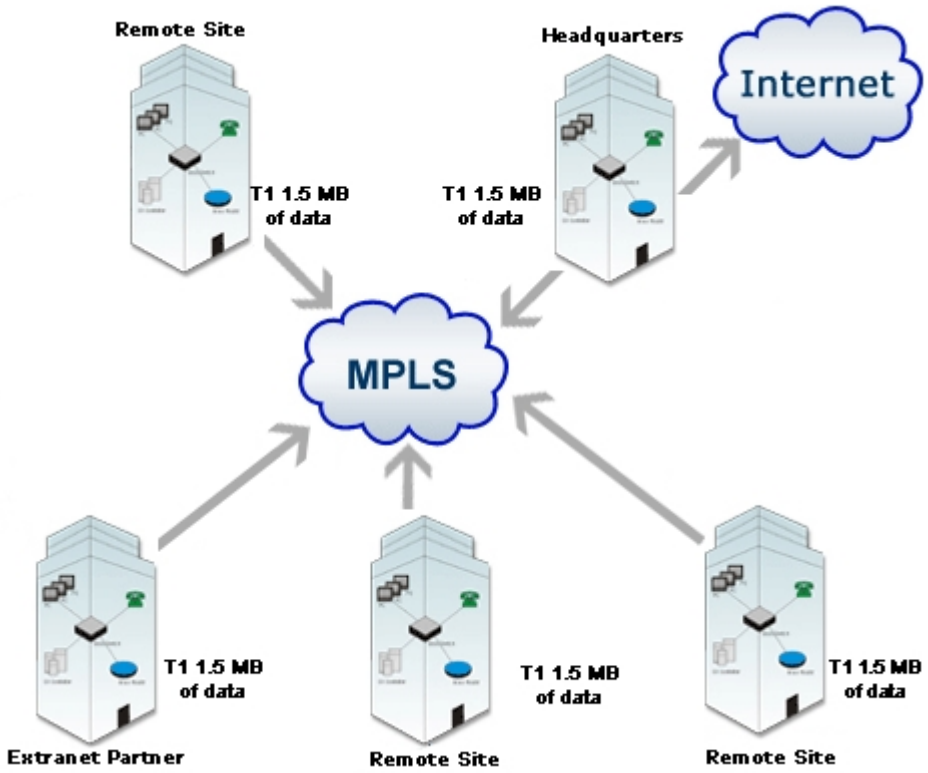
Asynchronous Transfer Mode

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 50

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 51

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 52

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.

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

Question 53

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).

Question 54

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 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.

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

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 55

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.

Question 56

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 57

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 58

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 59

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:

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

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 60

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

Question 61

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.

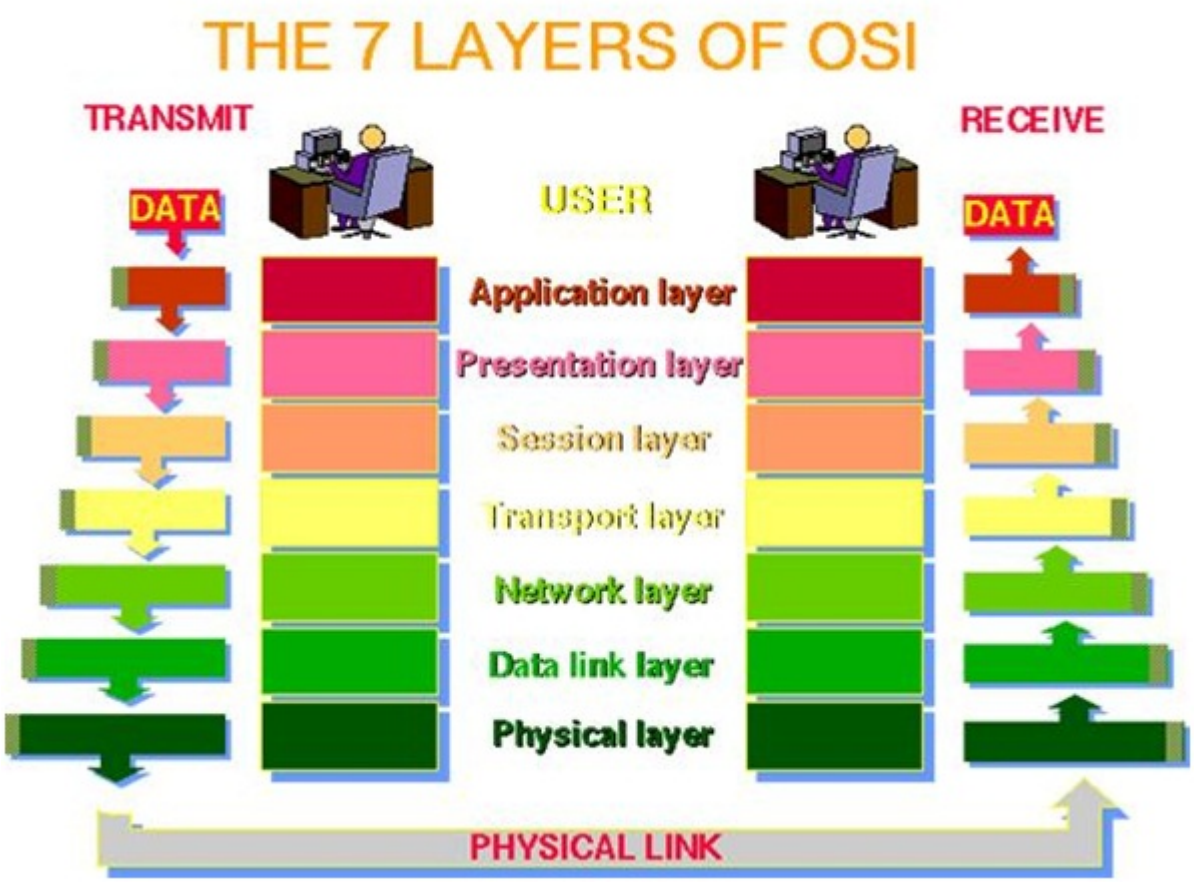
For your exam you should know below information about OSI model:

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.

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

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

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

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.

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 62

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 63

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

Question 64

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 65

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.

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

Question 66

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:

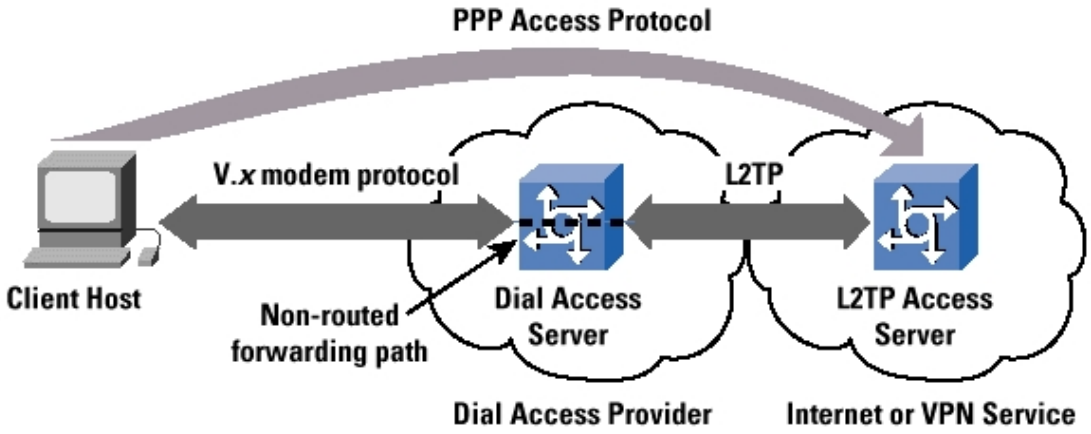
Point-to-point protocol

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.

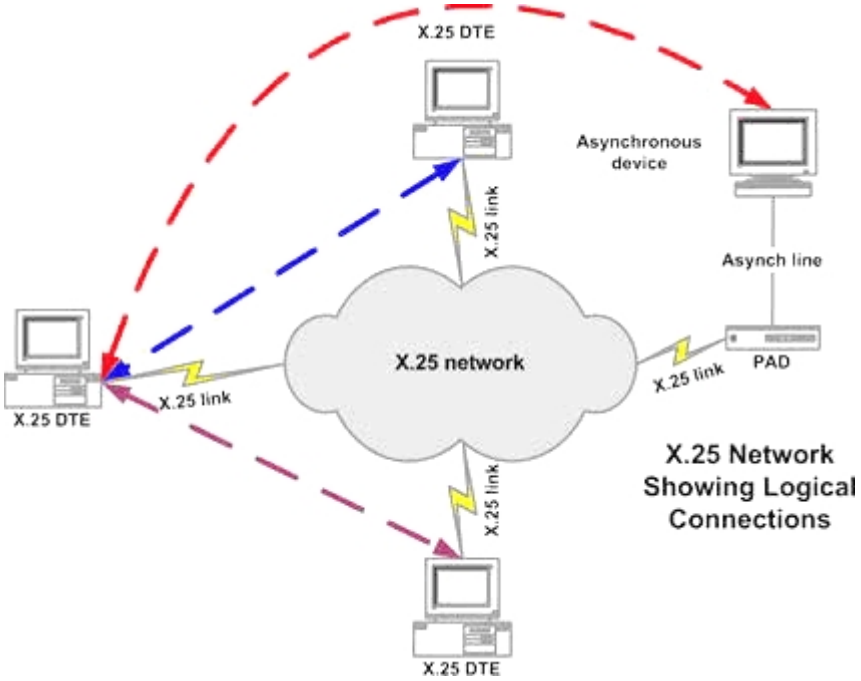
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

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

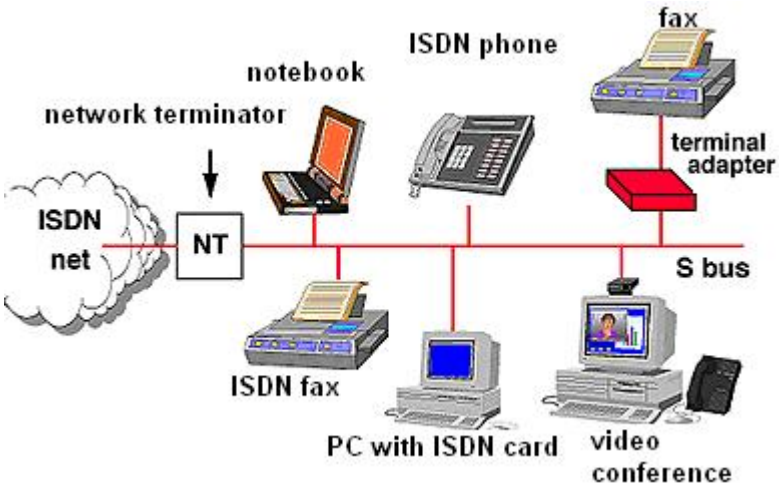
Licensed to Berend Post berend.post@it-university.nl

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

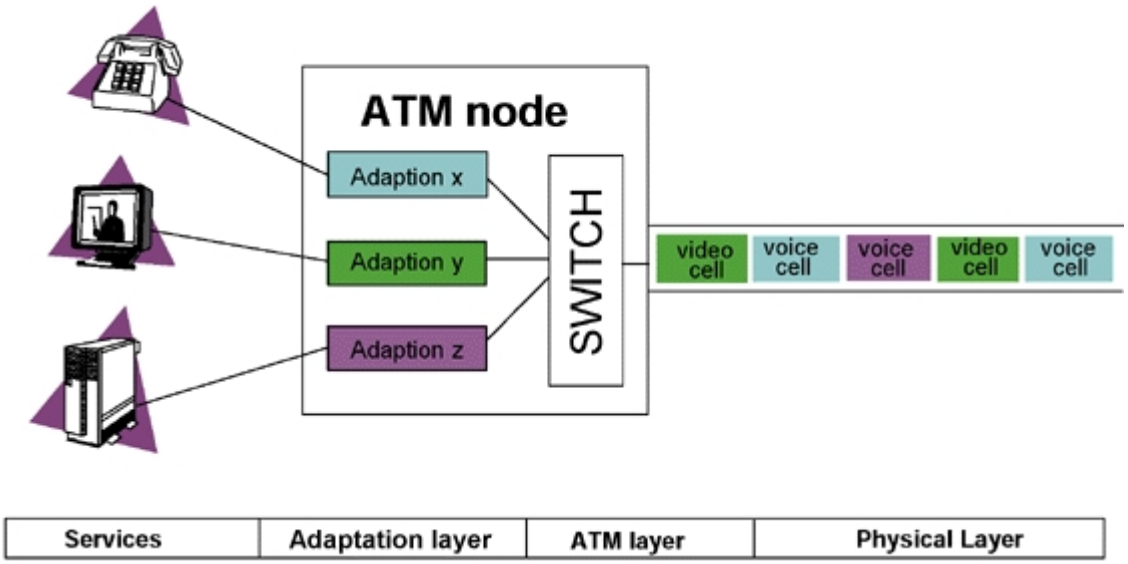
Like a frame relay it is connection oriented technology which creates and uses fixed channel

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

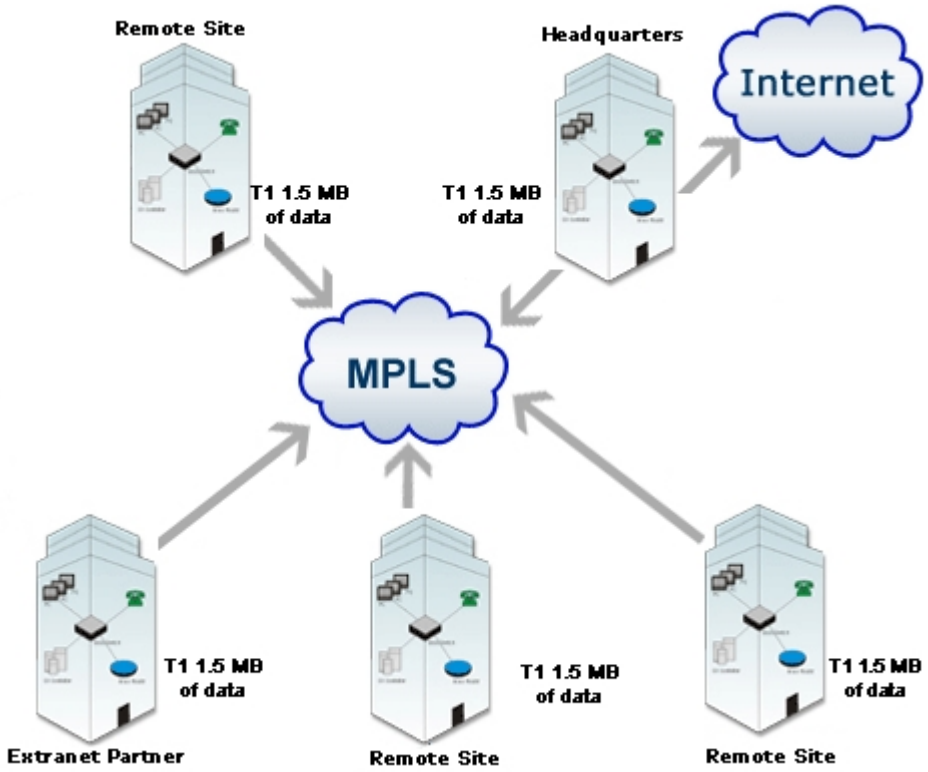


Multiprotocol Label Switching (MPLS)

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 67

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.

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

Question 68

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 69

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 70

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.

Question 71

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.

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

Question 72

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 73

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.

Question 74

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

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

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 75

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 76

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.

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

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:

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 77

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

Question 78

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.

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

Question 79

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 80

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 81

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 82

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 83

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.

Question 84

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:

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.

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

Question 85

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 86

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 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 87

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:

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

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 88

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

Question 89

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:

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 90

To effectively classify data, which of the following MUST be determined?

- ☐ Data controls
- ☒ Data ownership
- ☐ Data users
- ☐ Data volume

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

Question 91

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 92

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 93

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.

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

Question 94

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.

Question 95

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 96

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.

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

Question 97

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

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

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 CSA.

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

CISA review manual 2014 page number 61, 62 and 63

Question 98

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

Question 99

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:

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

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.

Question 100

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.

Question 101

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 102

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 103

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 104

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.

Question 105

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.

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

Question 106

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 107

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.

Quantify the probability and business impact of these potential threats.

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

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.

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

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

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 108

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

Question 109

Which of the following is the PRIMARY role of a data custodian?

- ☐ Processing information
- ☒ Securing information
- ☐ Classifying information
- ☐ Validating information

Question 110

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.

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

Question 111

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.

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 112

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.

Question 113

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 114

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:

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.

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

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

Question 115

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.

Question 116

The PRIMARY reason for using digital signatures is to ensure data:

- ☐ confidentiality.
- ☒ integrity.
- ☐ availability.
- ☐ timeliness.

Explanation:

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

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

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 117

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.

Question 118

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 119

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.

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

Question 120

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 121

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 122

An organization has implemented an automated match between purchase orders, good 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

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

Question 123

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 124

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 125

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:

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

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 126

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).

Question 127

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.

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

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.

Question 128

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 129

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 130

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

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

Question 131

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.

Question 132

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 133

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

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

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.

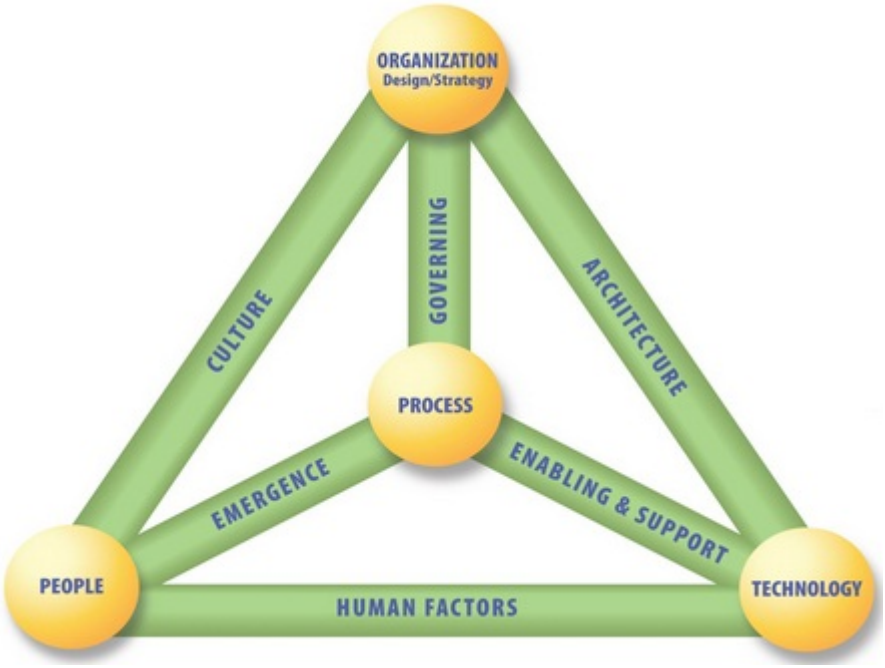
Business Model for Information Security

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 134

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 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

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 348

http://en.wikipedia.org/wiki/Honeypot_%28computing%29

Question 135

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 136

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 137

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 138

The BEST way to avoid session hijacking is to use:

- ☐ a reverse lookup
- ☒ a secure protocol
- ☐ a firewall
- ☐ strong password controls

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

Question 139

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

Question 140

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 141

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.

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

Question 142

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 143

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 144

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 145

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 146

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:

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

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 147

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.

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

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

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 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

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

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.

Question 148

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 149

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.

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

Question 150

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 151

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 152

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 153

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

Question 154

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 155

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

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

Question 156

Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?

- ☒ Balanced scorecards
- ☐ Benchmarking
- ☐ Maturity models
- ☐ Peer reviews

Question 157

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

Question 158

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

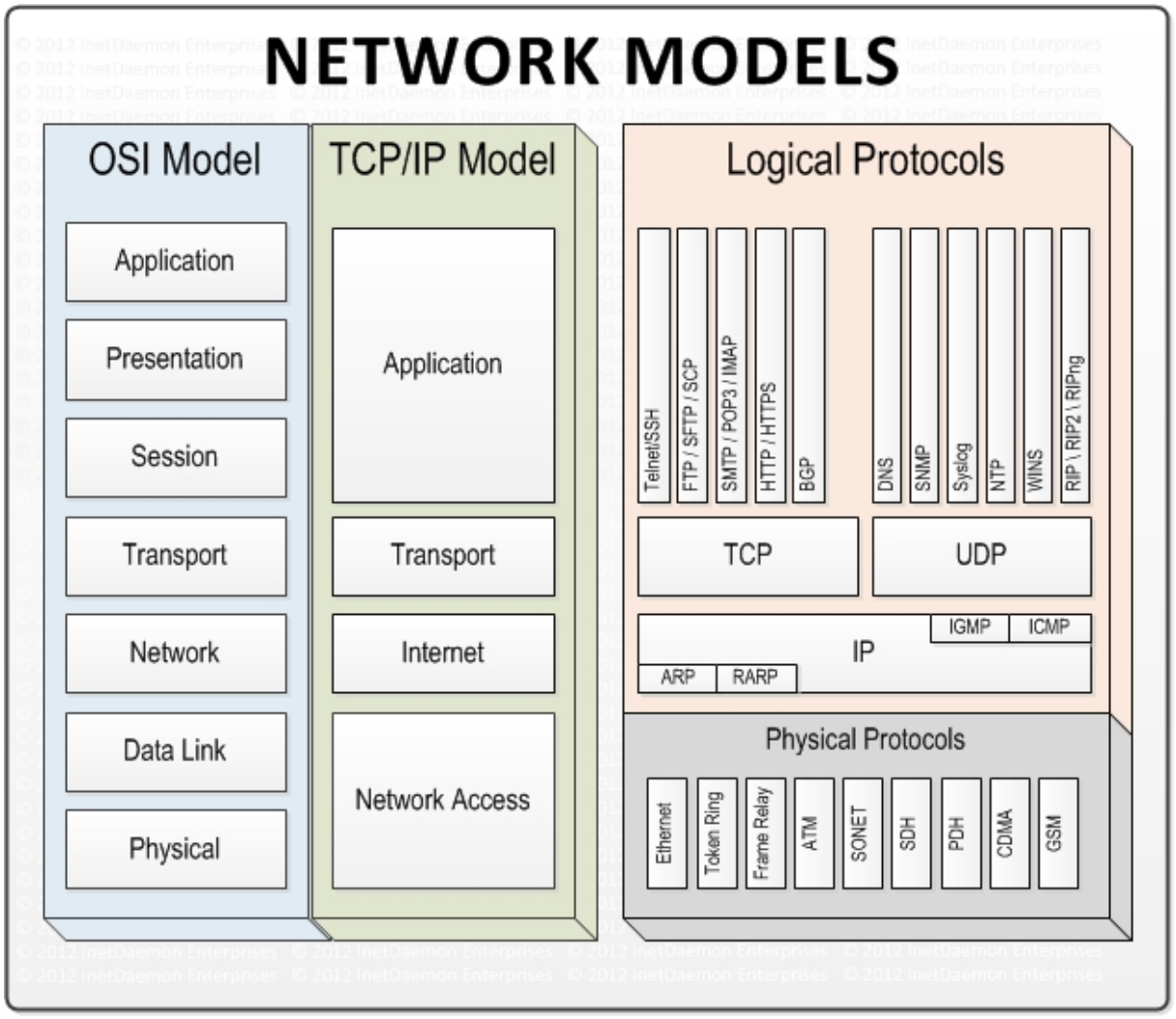
- ☐ Data
- ☒ Segment
- ☐ Packet
- ☐ Frame

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.

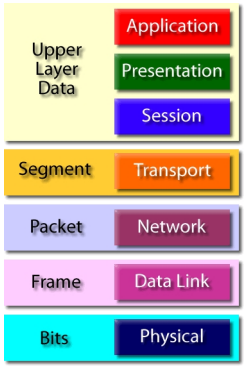
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the 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 159

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

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

key encryption for message encryption. Digital signature certificates are used by SSL for server authentication.

Question 160

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)

Question 161

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 162

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 163

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 164

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 165

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:

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.

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

Question 166

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.

Question 167

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 168

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

Question 169

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 170

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 171

In an EDI process, the device which transmits and receives electronic documents is the:

- ☒ communications handler.
- ☐ EDI translator.
- ☐ application interface.
- ☐ EDI interface.

Explanation:

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

Question 172

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 173

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 174

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 175

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 176

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 177

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:

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 178

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 179

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.

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

Question 180

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

Question 181

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."

Question 182

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.

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

Question 183

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:

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 184

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.

Question 185

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

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

Question 186

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:

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 187

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 188

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

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

an all-or- nothing proposition. The client will accept the program if the parameters are established to do so.

Question 189

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 190

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 191

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 192

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.

Question 193

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

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

Question 194

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 195

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 196

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.

Question 197

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.
- ☐ 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:

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

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

enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

Question 198

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 199

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

Question 200

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

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

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 201

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 202

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 203

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 204

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:

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

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 205

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

Question 206

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 207

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.

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

Question 208

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 209

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 210

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.

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

Question 211

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.

Question 212

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 213

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

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

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 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.

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

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

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

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

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 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

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

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.

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

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

Question 214

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 215

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.

Question 216

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 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

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

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 217

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.

Question 218

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

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

Question 219

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.

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 220

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 221

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 222

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.

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

Question 223

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.

Question 224

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 225

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 226

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:

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

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.

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.

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

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

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

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

http://howdoesinternetwork.com/2013/jitter

Question 227

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 processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

Question 228

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.

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

Question 229

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 230

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:

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

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.

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.

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

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.

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.

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

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

Question 231

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 232

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 233

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 234

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 235

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

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

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 236

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 237

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 238

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.

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

Question 239

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.

Question 240

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.

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

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.

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.

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

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:

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 241

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:

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

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 242

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 243

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.

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

Question 244

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.

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:

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.

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 245

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 246

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 247

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:

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

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 248

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 249

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 250

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.

Question 251

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.

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

Question 252

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

Question 253

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 254

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 255

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 256

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 257

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:

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

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.

Question 258

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 259

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:

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.

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

Question 260

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 261

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

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

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.

Question 262

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.

Question 263

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 264

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,

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

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.

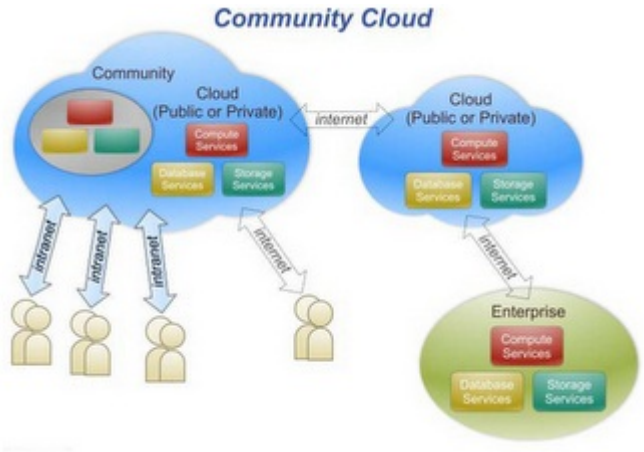
Private Cloud

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

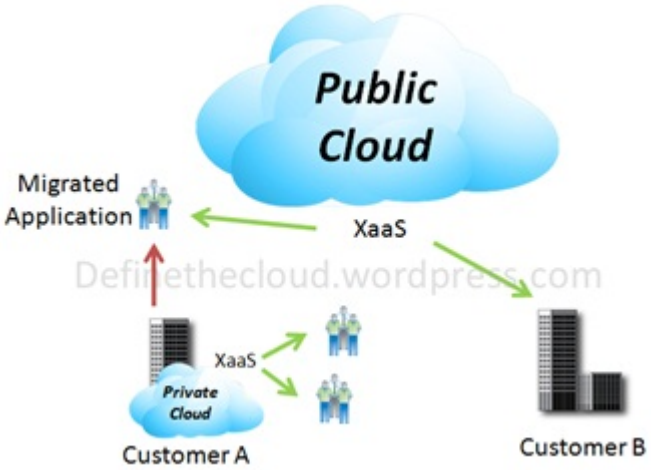
Licensed to Berend Post berend.post@it-university.nl



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

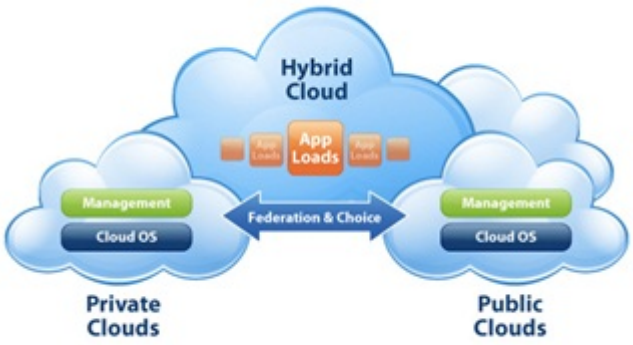


Hybrid cloud

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.

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

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

Question 265

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 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 266

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.

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

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.

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.

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

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:

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 267

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 268

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.

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

Question 269

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 270

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 271

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 272

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 273

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.

Question 274

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 275

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 276

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 277

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

Question 278

Which of the following is the BEST type of backup to minimize the associated time and media?

- ☒ Differential
- ☐ Incremental
- ☐ Mirror
- ☐ Compressed full

Question 279

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 280

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.

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

Question 281

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 282

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 283

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:

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.

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

Question 284

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 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 285

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 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.

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

Question 286

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 287

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.

Question 288

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.

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

Question 289

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.

Question 290

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 291

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

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

Question 292

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 293

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

Question 294

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

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

Question 295

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

Question 296

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 297

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 298

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.

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

Question 299

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 300

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 301

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 302

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

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

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 303

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 304

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:

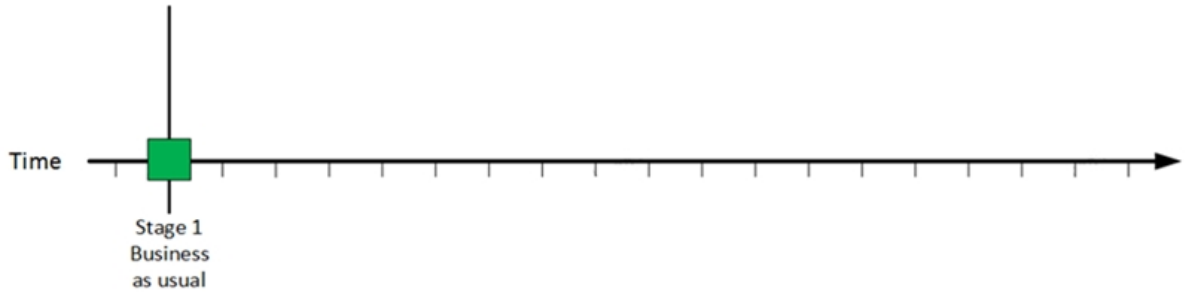
The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed 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

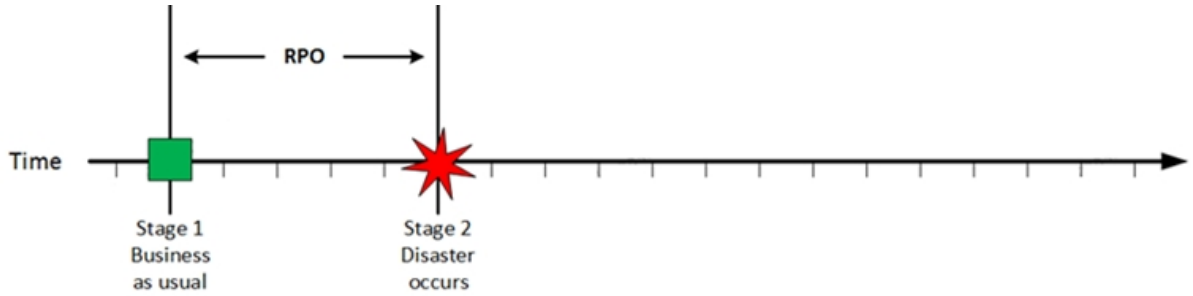
Licensed to Berend Post berend.post@it-university.nl



At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

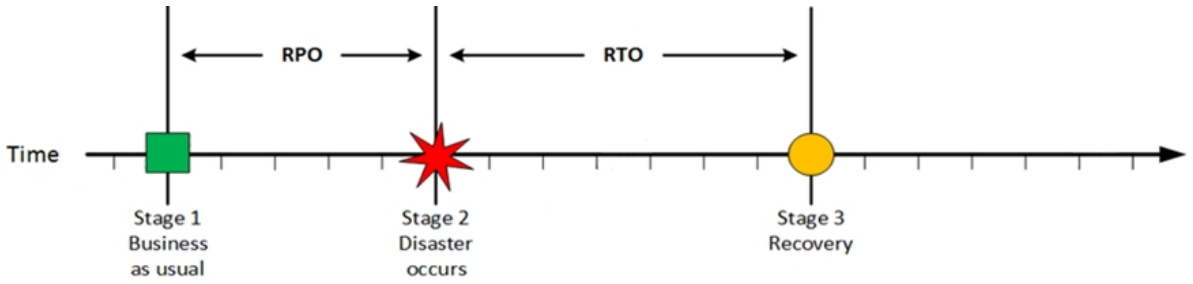
Disaster Occurs



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

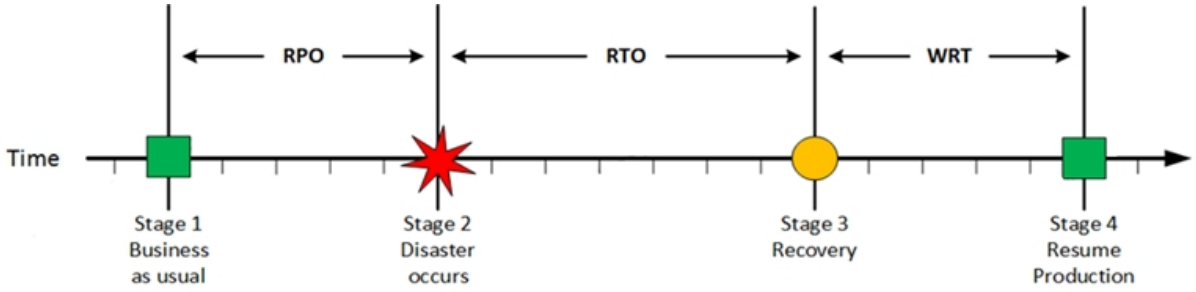


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

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

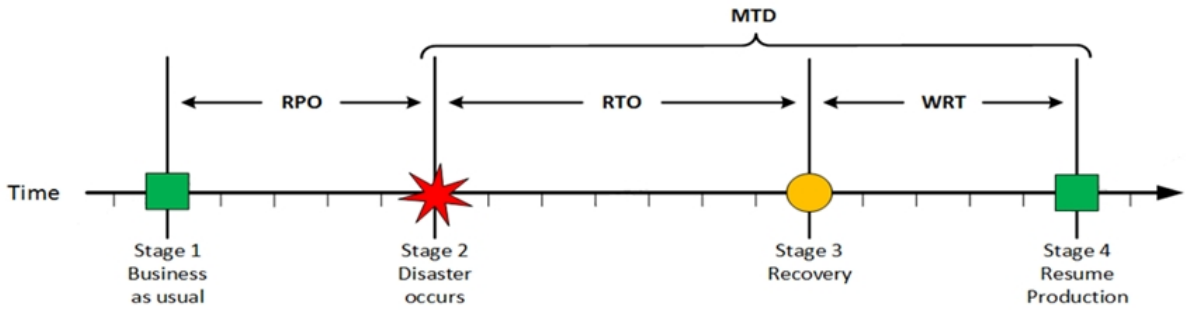
Stage 4: Resume Production

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:

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

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.

References:

CISA review manual 2014 page number 284

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 305

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.

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

Question 306

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.

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.

Radio System

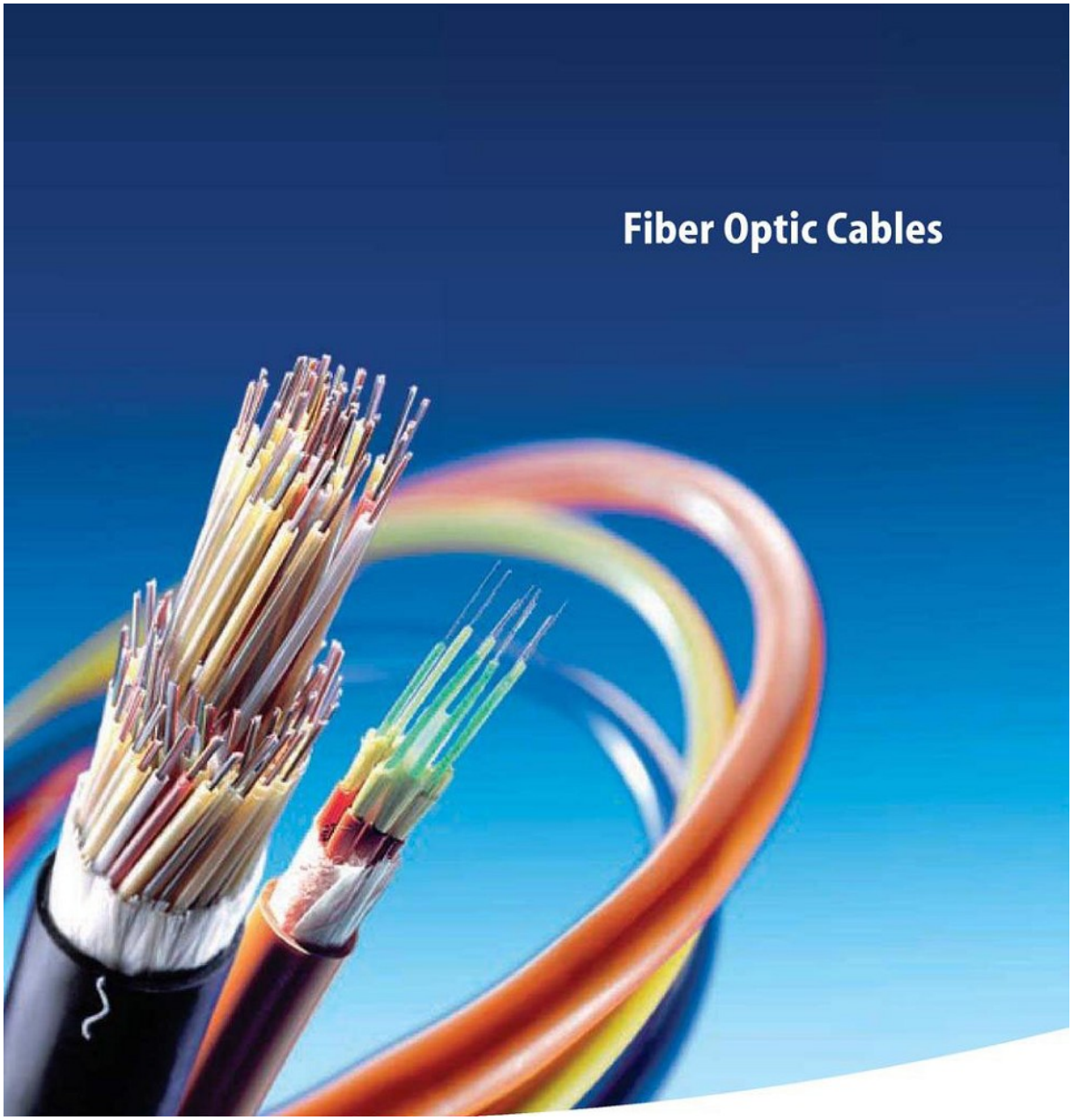
Radio systems are used for short distance, cheap and easy to tap.

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.

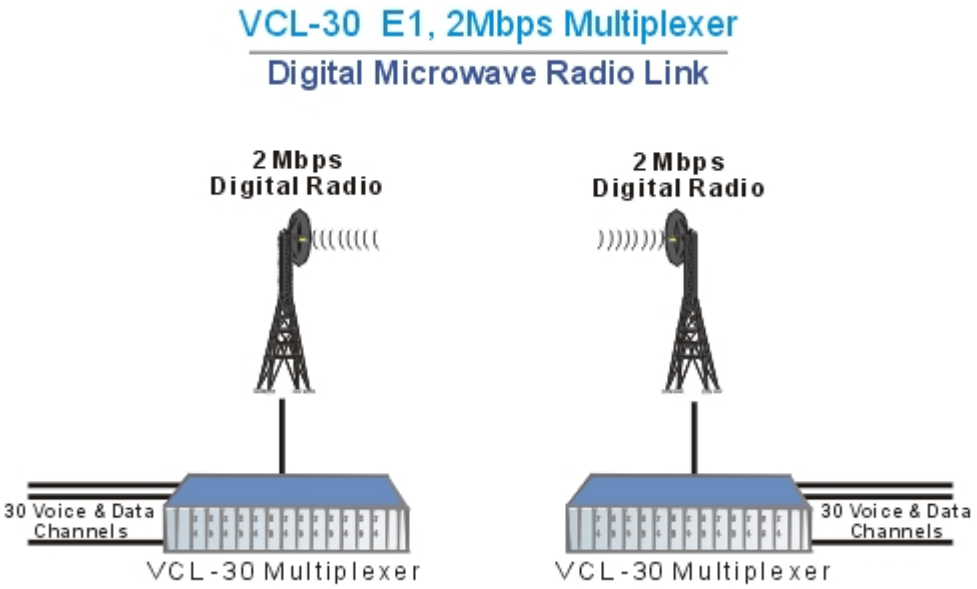
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering 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 307

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 308

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 309

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 310

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:

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 311

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 312

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:

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

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.

Question 313

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.

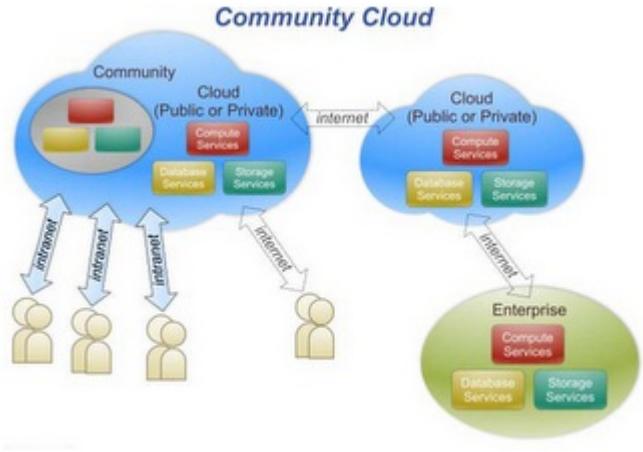
Private Cloud

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

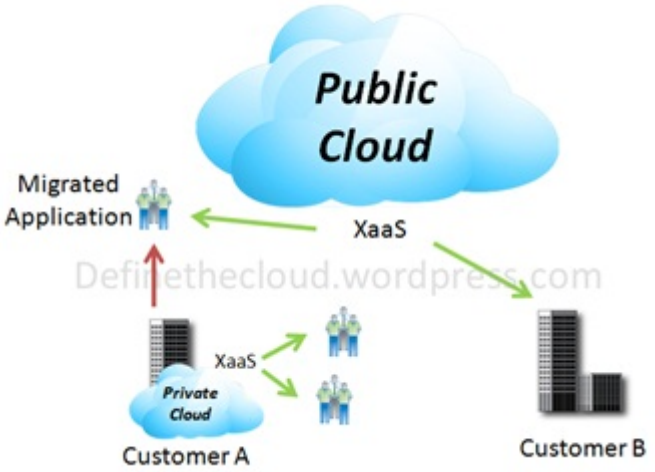


Public Cloud

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

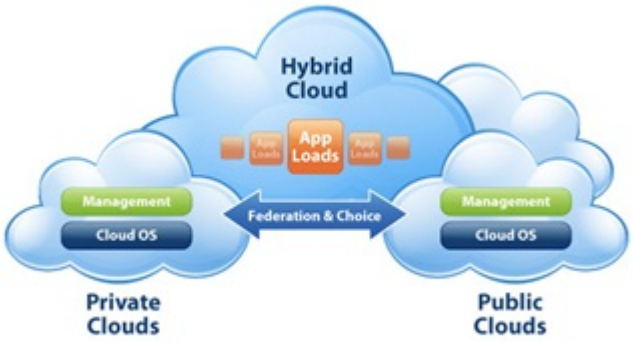
Licensed to Berend Post berend.post@it-university.nl



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

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

Question 314

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?

- ☐ Calculated the return on investment (ROI).
- ☐ Interview stakeholders.
- ☒ Conduct an earned value analysis (EVA).
- ☐ Survey end users.

Question 315

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

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

Question 316

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:

Network performance-monitoring tools are used to measure and ensure proper network capacity management and availability of services.

Question 317

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.

Question 318

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 319

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

Question 320

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

Question 321

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

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

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.

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:

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

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

Question 322

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 323

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.

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

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.

Tunnel and Transport Modes

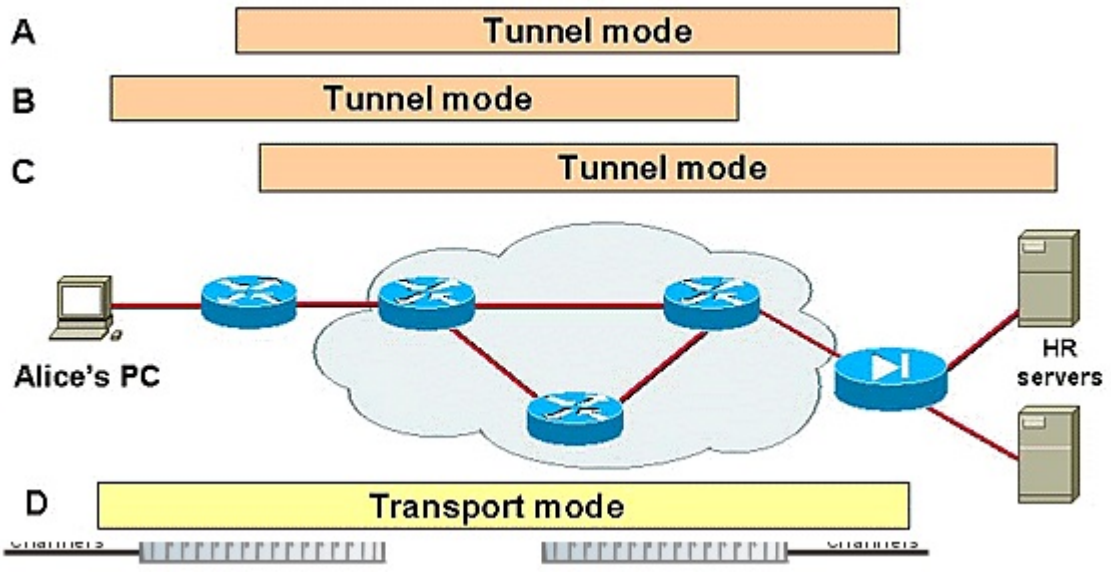
IPSec can be run in either tunnel mode or transport mode. Each of these modes has its own particular uses and care should be taken to ensure that the correct one is selected for the solution:

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

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

Tunnel and transport modes in IPSec.

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

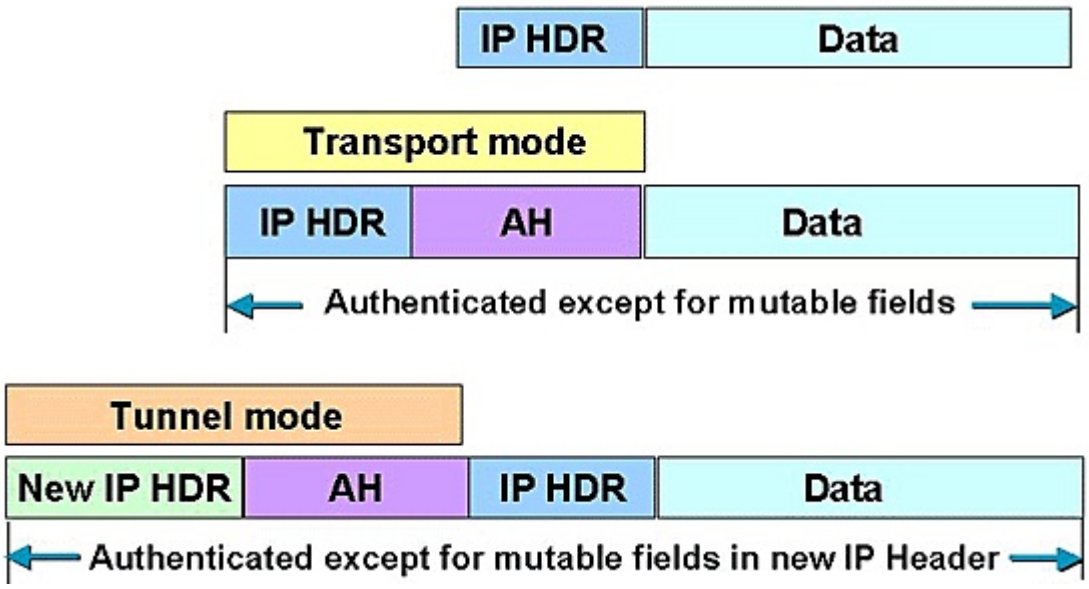
Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall (as shown in example A in Figure 1). The IPSec gateways proxy IPSec for the devices behind them, such as Alice's PC and the HR servers in Figure 1. In example A, Alice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

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

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

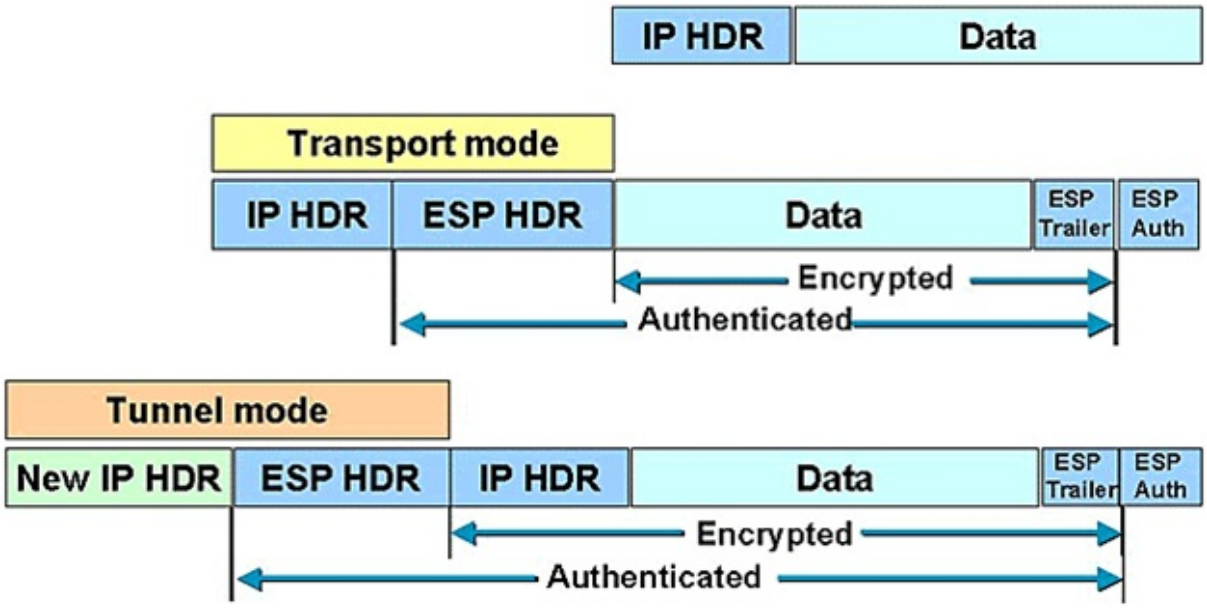
Figure 2 above, shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that don't change in transport. The header goes after the IP header and before the ESP header,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

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.

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

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.

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

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

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

and

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

Question 324

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 325

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:

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

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

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 326

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 327

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 328

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:

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 329

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.

Question 330

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:

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

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.

Question 331

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 332

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

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

Question 333

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 334

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 335

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 336

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 337

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)

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

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

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 338

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

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

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 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 339

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:

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

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

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 340

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.

Question 341

The MOSTimportant objective of security awareness training for business staff is to:

- ☐ understand intrusion methods
- ☐ reduce negative audit findings
- ☐ increase compliance
- ☒ modify behavior

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

Question 342

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 343

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.

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

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.

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

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

Question 344

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 345

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)

Question 346

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:

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.

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

Question 347

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 348

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.

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

Question 349

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 350

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.

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

Question 351

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.

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

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

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:

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

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

Question 352

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.

Question 353

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 354

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 355

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.

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

Question 356

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 357

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 358

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.

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

Question 359

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."

Question 360

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

Question 361

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.

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

Question 362

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

Question 363

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.

Question 364

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 365

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.

Question 366

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

Question 367

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 368

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 369

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 370

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

Question 371

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:

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

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.

Question 372

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 373

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

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

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

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 374

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 375

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:

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

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.

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.

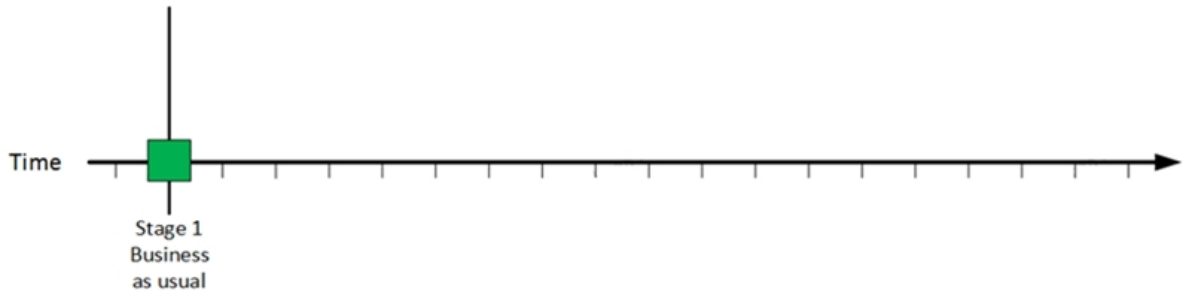
The RTO attaches to the business process and not the resources required to support the process.

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

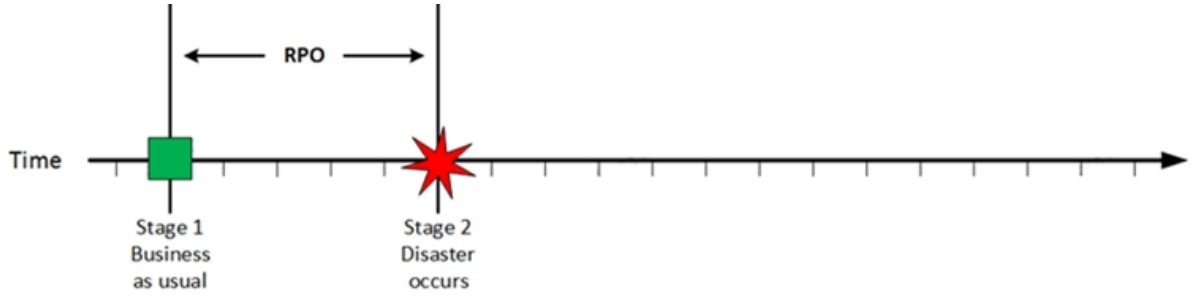


At this stage all systems are running production and working correctly.

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

Stage 2: Disaster occurs

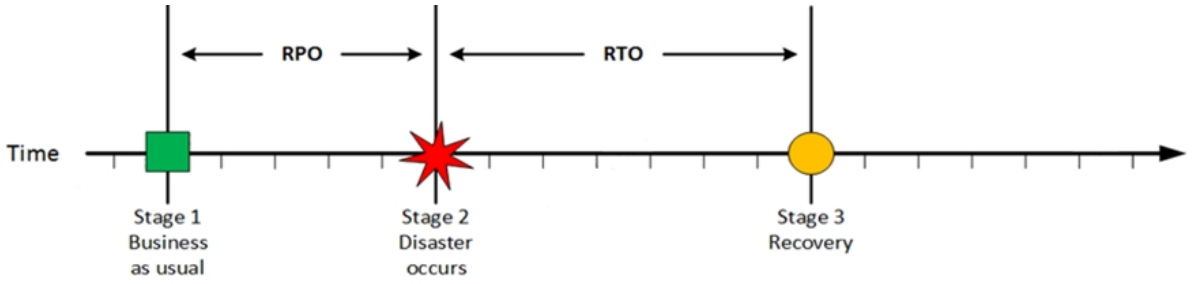
Disaster Occurs



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

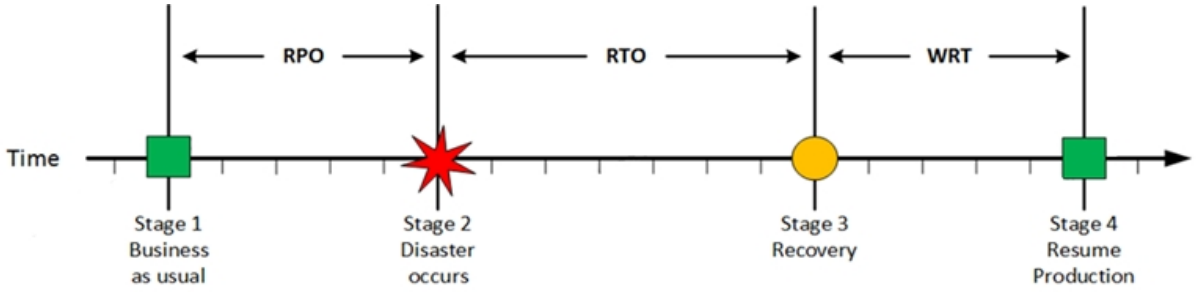


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

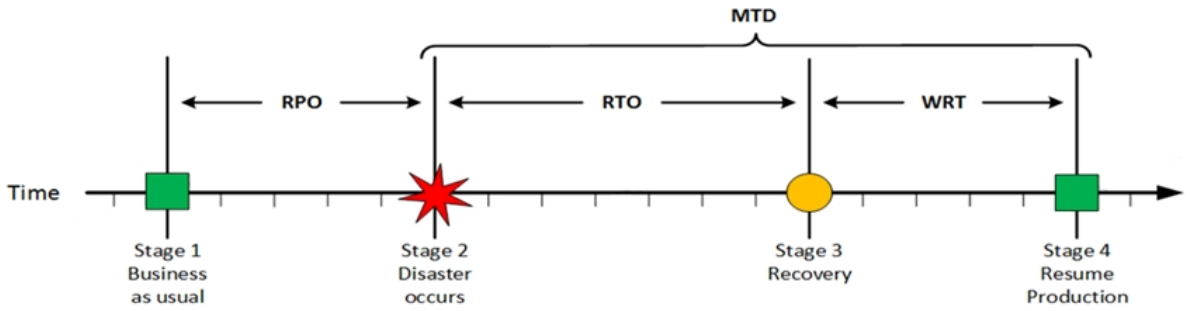
Resume Production

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.

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

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

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_time_objective

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 376

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 377

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 378

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.

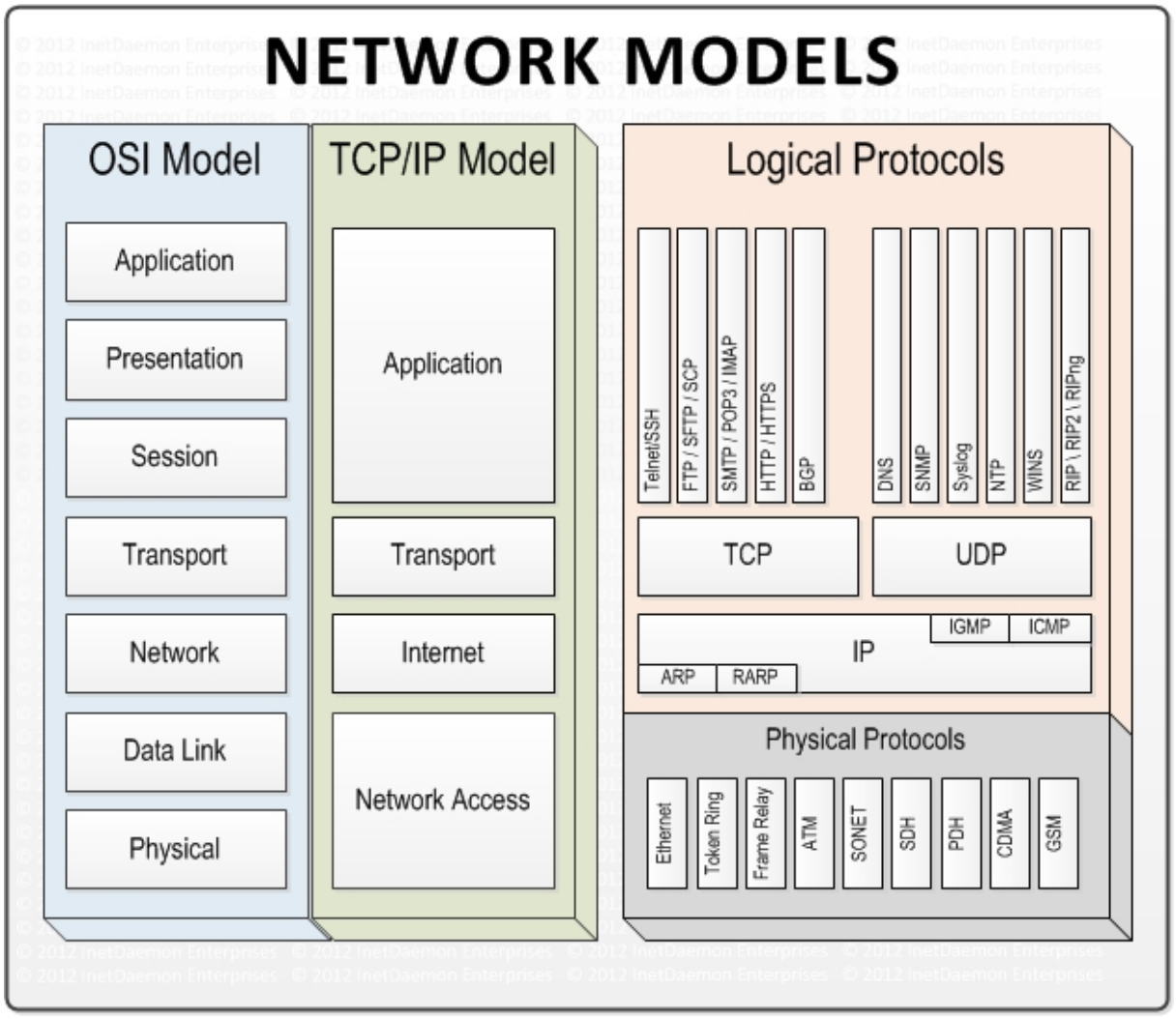
You need to find out invalid layer-protocol mapping.

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.

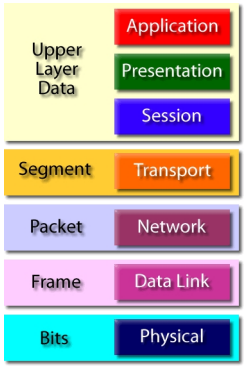
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the 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 379

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 380

Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

- ☒ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Explanation:

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

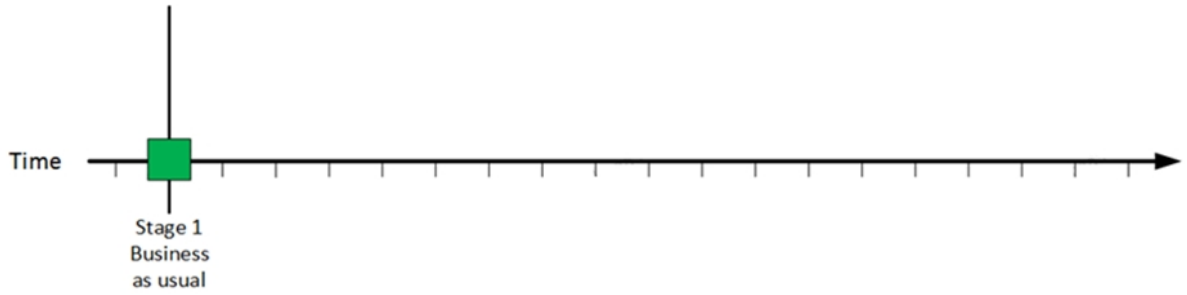
Explanation:

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

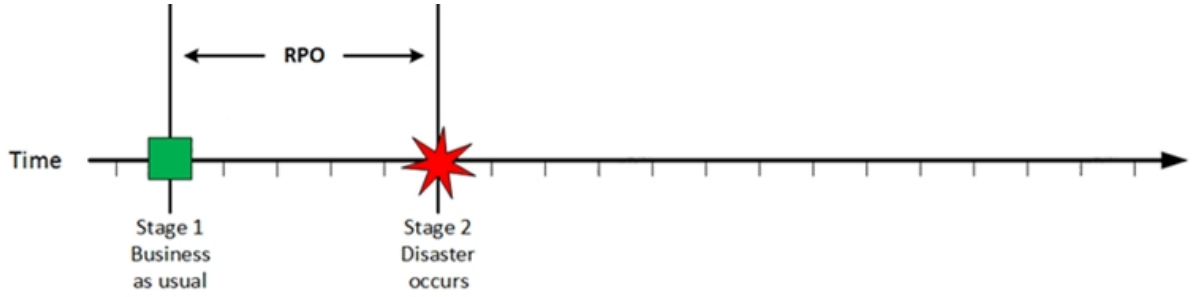


At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

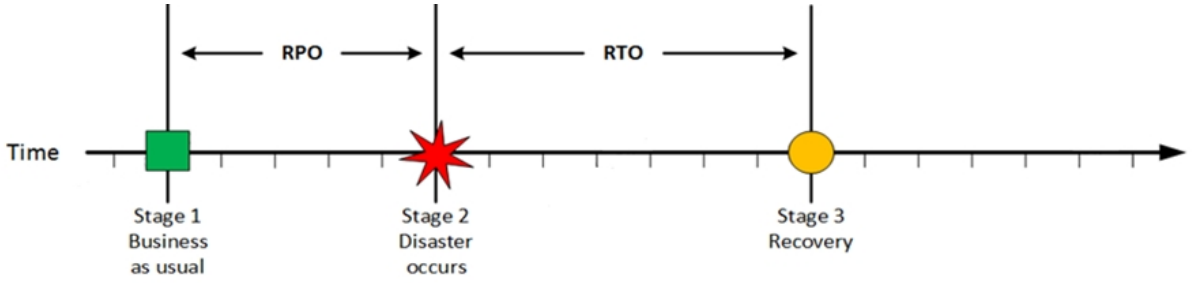
Licensed to Berend Post berend.post@it-university.nl



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

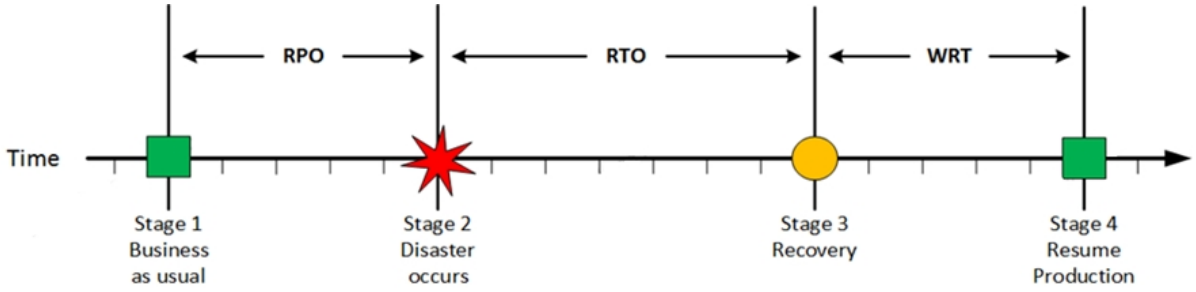


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

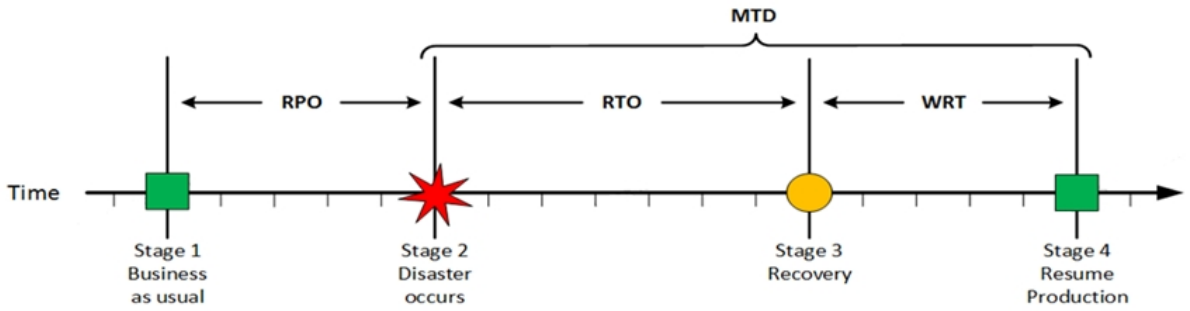
Resume Production

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:

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 381

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 382

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:

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

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 383

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 384

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 385

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:

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

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 386

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.

Question 387

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.

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

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

Question 388

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 389

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:

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

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.

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

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

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:

CISA review manual 2014 Page number 167

Question 390

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:

Explanation:

Lack of employee awareness of a company's information security policy could lead to an unintentional loss of confidentiality.

Question 391

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

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

Question 392

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 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 393

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

Question 394

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

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 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

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

Question 395

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 would be 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 396

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 397

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 398

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 399

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 400

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.

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

Question 401

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 402

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 403

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

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

Question 404

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

Question 405

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.

Question 406

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.

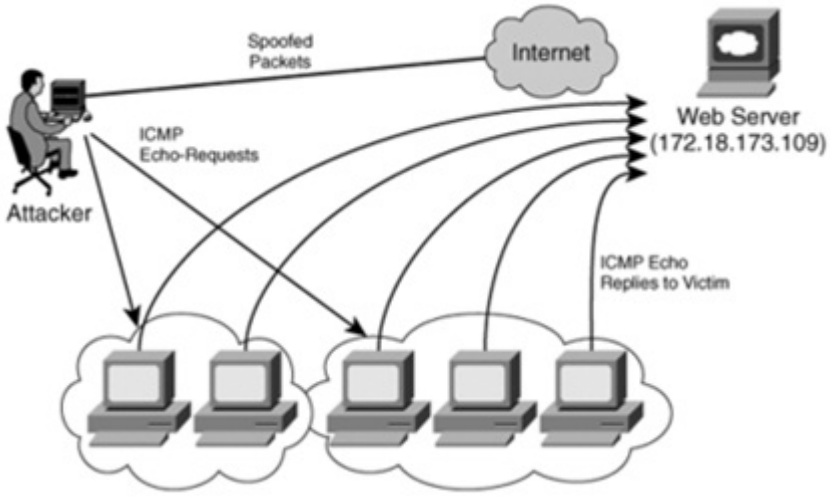
A distributed denial of service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. (This reflected attack form is sometimes called a "DRDOS".

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

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.

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

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

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 407

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

 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 408

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.

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

Question 409

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 410

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 411

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

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

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.

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

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

Question 412

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 413

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Allowing application programmers to directly patch or change code in production programs increases risk of fraud.

Question 414

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 415

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.

Question 416

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 417

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.

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

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.

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

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

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

Question 418

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

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

of controls within the layers mentioned above along with known vulnerabilities within the database software.

Question 419

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.

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 420

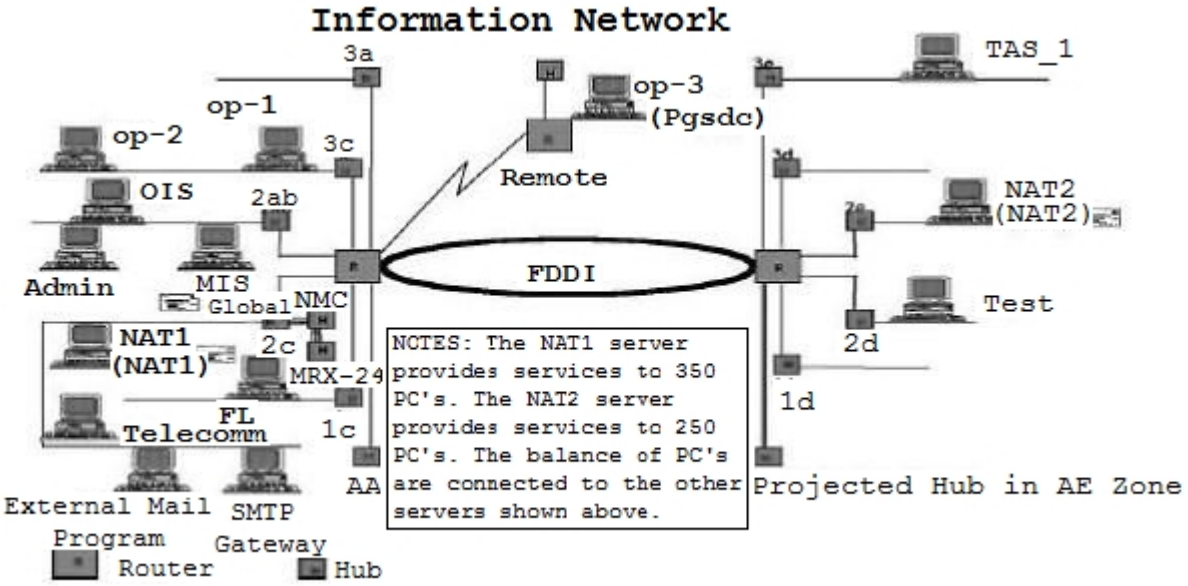
A small organization is experiencing rapid growth and plans to create a new information security policy. Which of the following is MOST relevant to creating the policy?

- ☐ Industry standards
- ☐ The business impact analysis
- ☒ The business objectives
- ☐ Previous audit recommendations

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

Question 421

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:

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 422

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

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

Question 423

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.

Question 424

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. Seas is closely related to the ASP (application service provider) and on demand computing software delivery models.

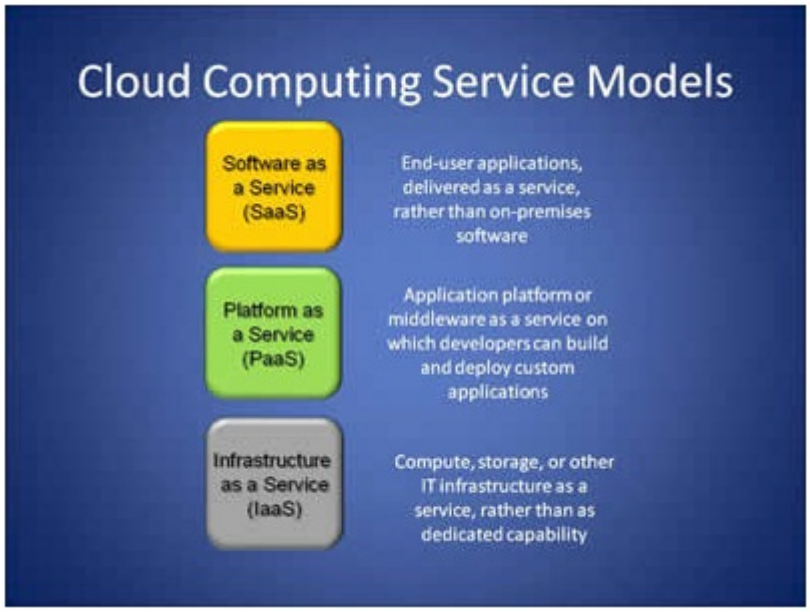
For your exam you should know below information about Cloud Computing:

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

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 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)

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

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

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

Question 425

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 426

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.

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:

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.

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.

Question 427

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 428

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 429

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.

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 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 430

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 431

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.

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

Question 432

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 433

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 434

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.

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

Question 435

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 436

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.

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

Question 437

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)

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:

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.

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 438

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.

Question 439

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.

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

Question 440

Which of the following are valid examples of Malware:

- ☐ viruses
- ☐ worms
- ☐ trojan horses
- ☐ spyware
- ☒ All of the above

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.

Question 441

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 442

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:

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

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.

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

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

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).

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 443

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.

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

Question 444

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 445

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.

Question 446

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:

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

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):

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:

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:

CISA review manual 2014 page number 275

Question 447

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.

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

Question 448

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 449

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.

Question 450

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 451

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 452

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.

Question 453

The FIRST step in data classification is to:

- ☒ establish ownership.
- ☐ perform a criticality analysis.
- ☐ define access rules.
- ☐ create a data dictionary.

Explanation:

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

Explanation:

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 454

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 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 455

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.

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

Question 456

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.

Question 457

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 458

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 459

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 460

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 461

Which of the following is protocol data unit (PDU) of network interface layer in TCP/IP model?

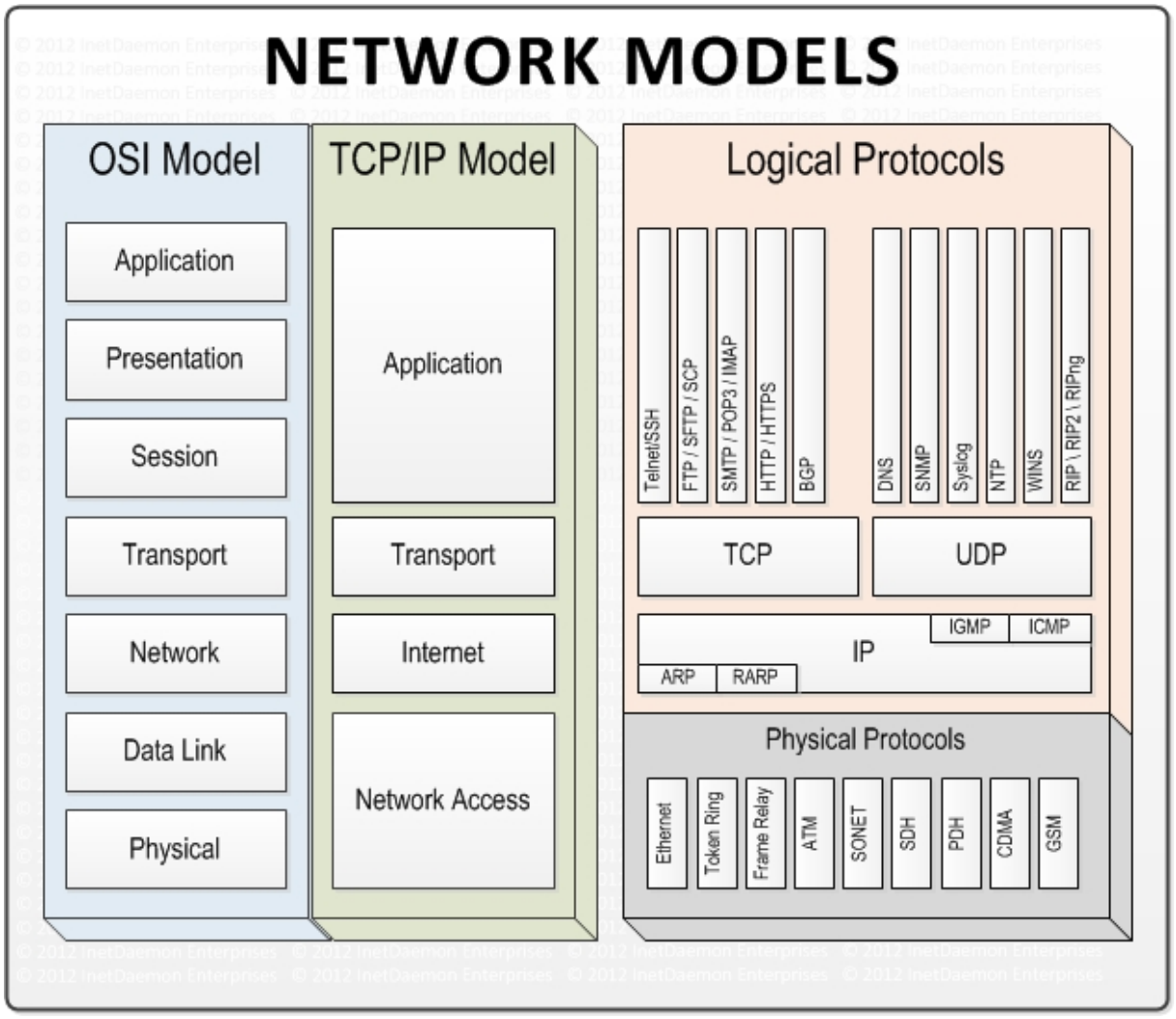
- ☐ Data
- ☐ Segment
- ☒ Packet
- ☐ Frame

Explanation:

For your exam you should know below information about TCP/IP model:

Network models

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.

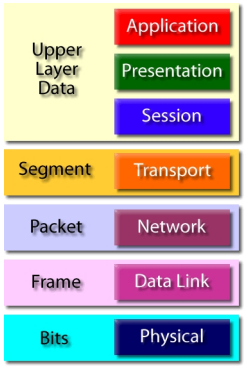
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the 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

Segment – Transport 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 462

Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☒ TCP

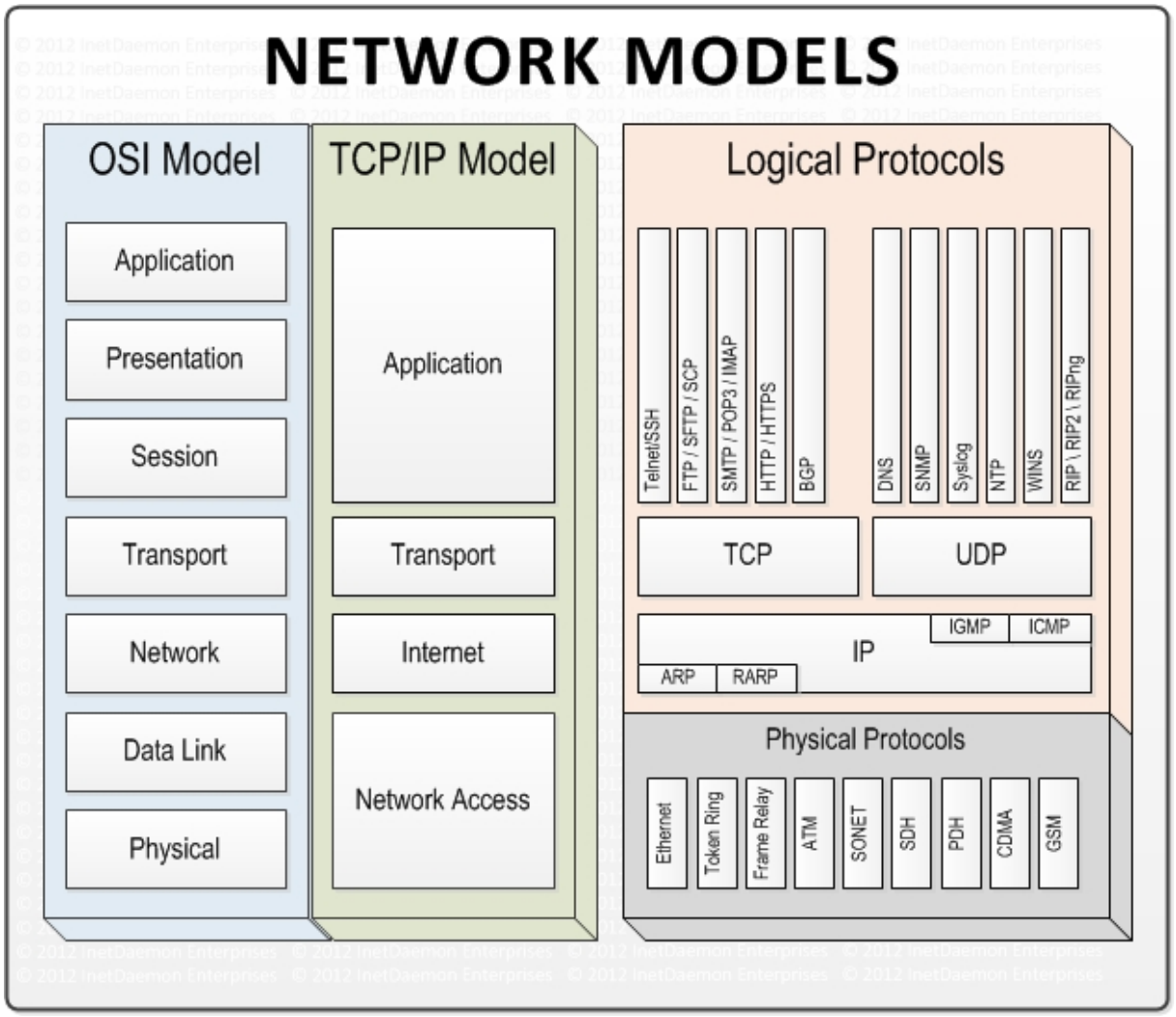
Explanation:

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:

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

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.

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

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

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.

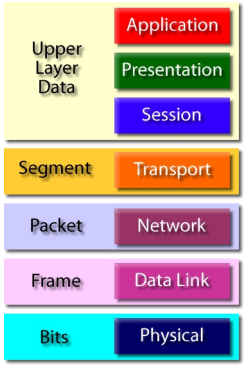
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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:

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

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

Question 463

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:

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 464

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

Question 465

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:

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.

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

Question 466

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 467

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 468

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 469

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 470

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.

Question 471

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.

Question 472

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 473

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

Question 474

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 475

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.

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

Question 476

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, 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.

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

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 477

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 478

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.

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

Question 479

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 480

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 481

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 482

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:

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

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 483

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 484

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 485

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 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.

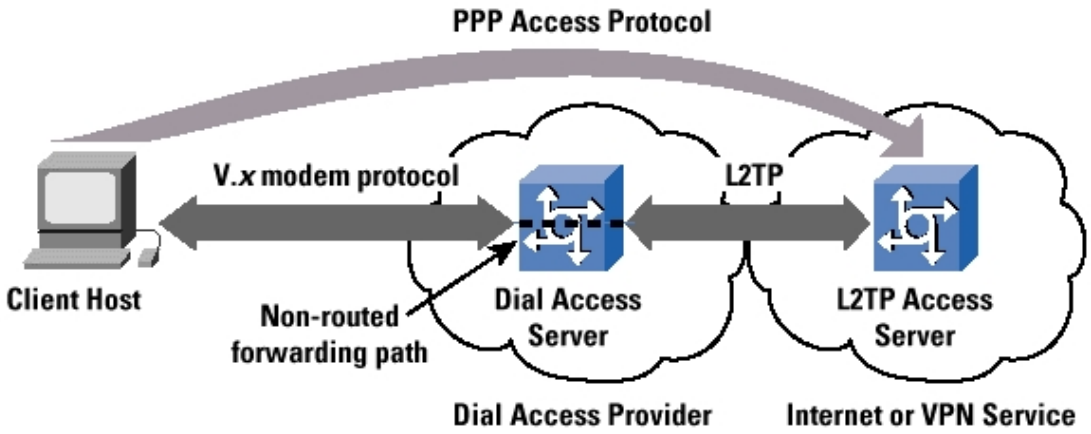
PPP uses the Internet protocol (IP) (and is designed to handle other protocol as well). It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your 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

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



X.25

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

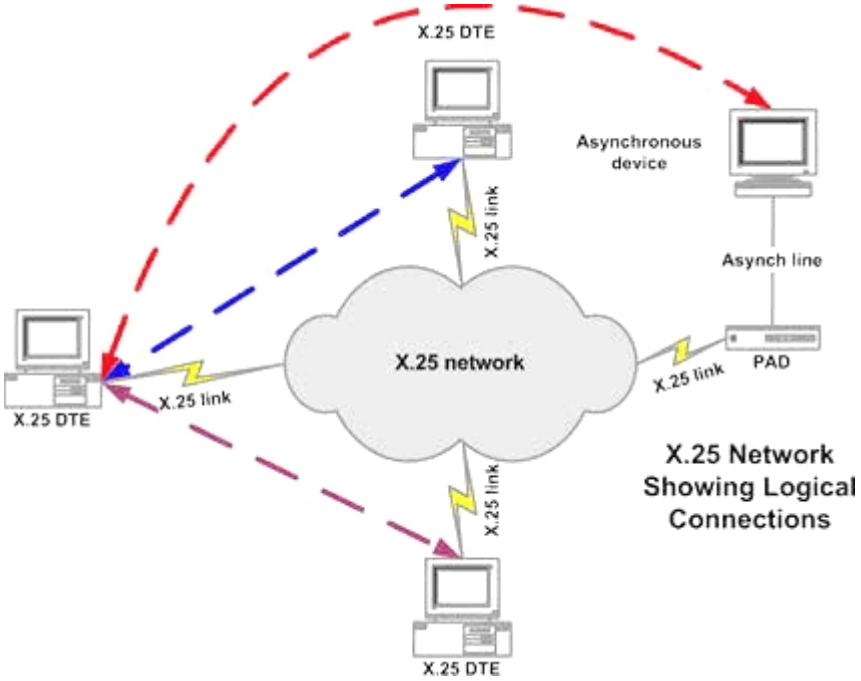
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

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 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

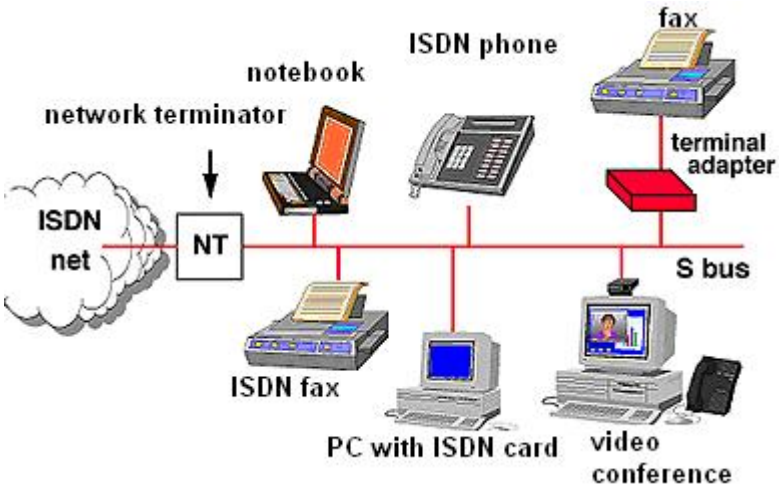
1. Data Terminal Equipment (DTE) - Usually a customer owned device that provides connectivity between company's own network and the frame relay's network.

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



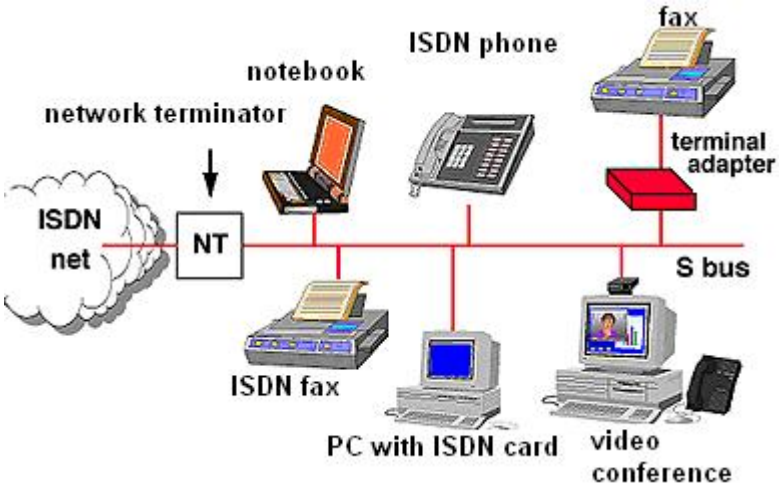
Integrated Service Digital Network (ISDN)

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



Asynchronous Transfer Mode (ATM)

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

Uses Cell switching method

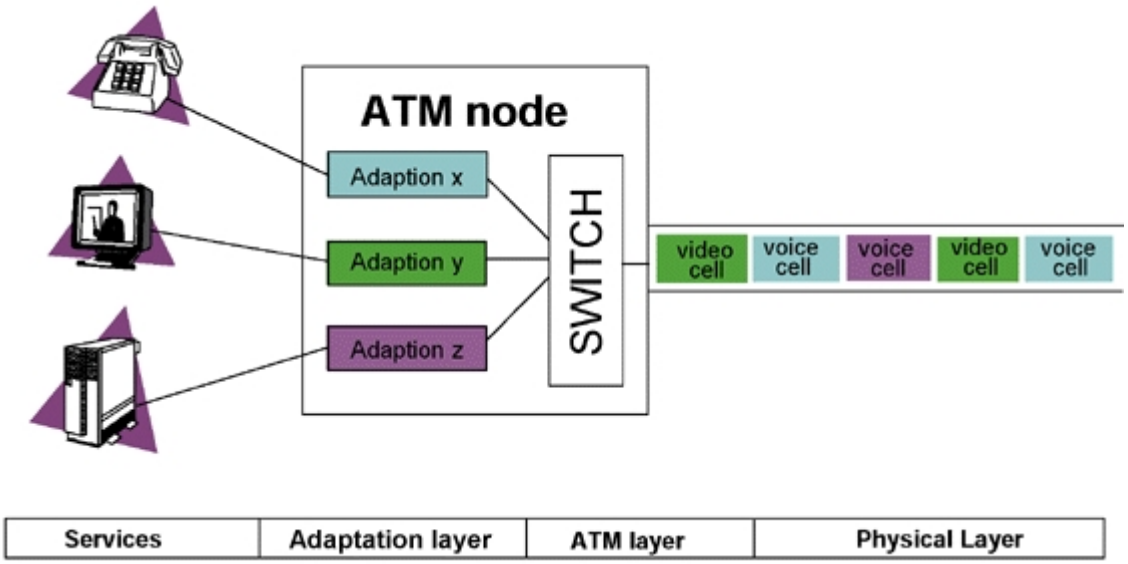
High speed network technology used for LAN, MAN and WAN

Like 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 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.

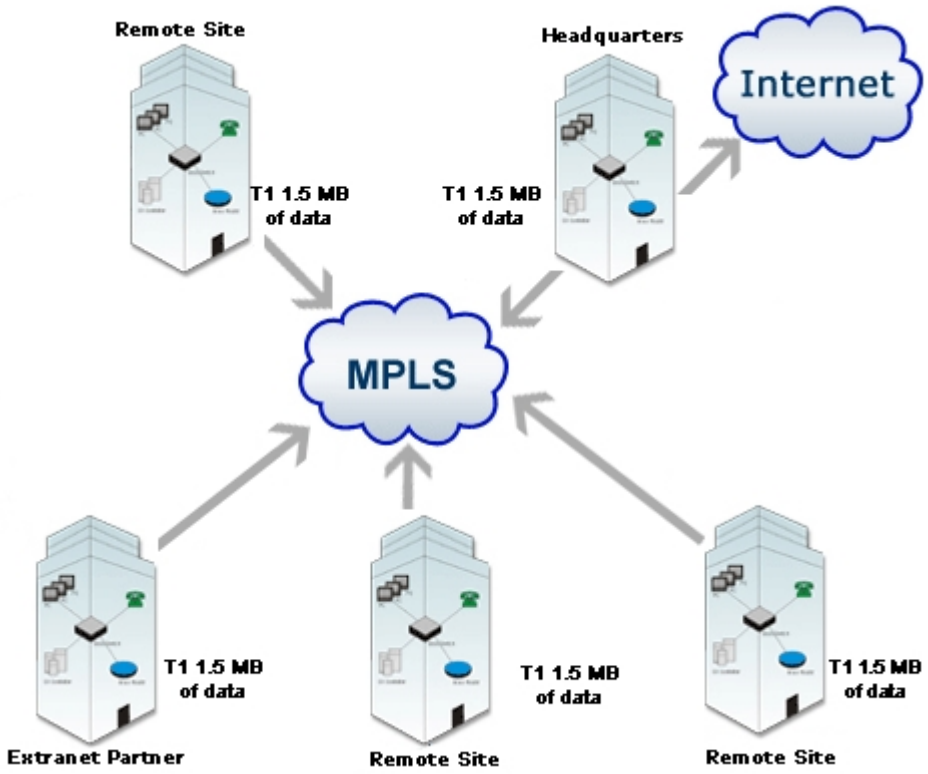
MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols.

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.

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

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

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 486

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 487

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:

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 488

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.

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

Question 489

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:

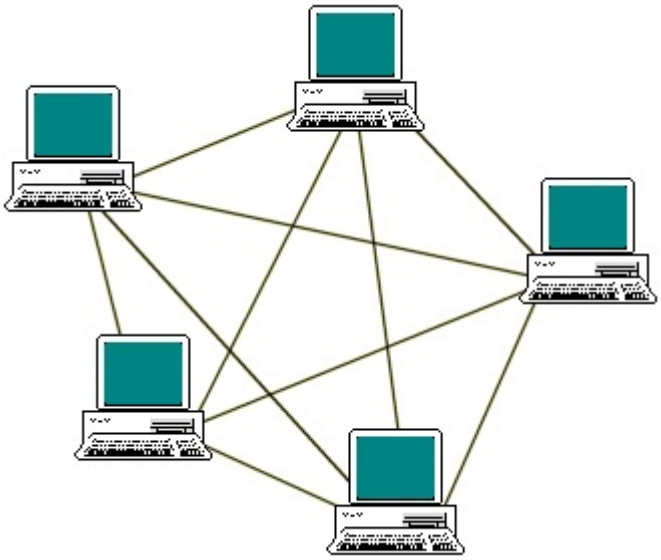
CISA review manual 2014 Page number 350 and 351

http://en.wikipedia.org/wiki/Public-key_cryptography

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

Question 490

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 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.

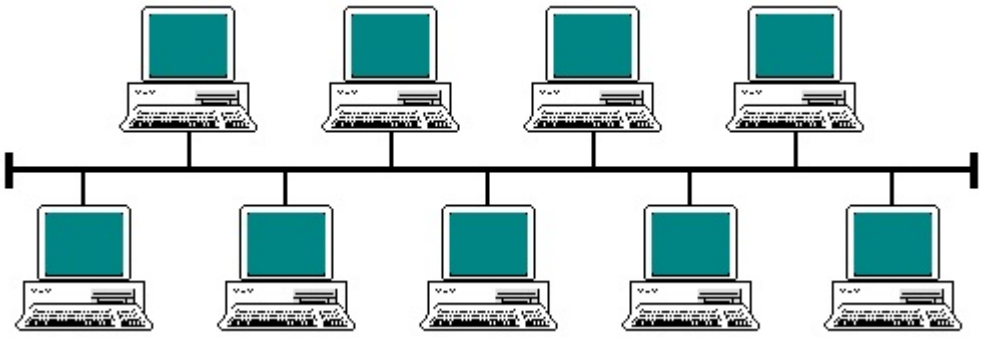
Bus

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

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

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 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.

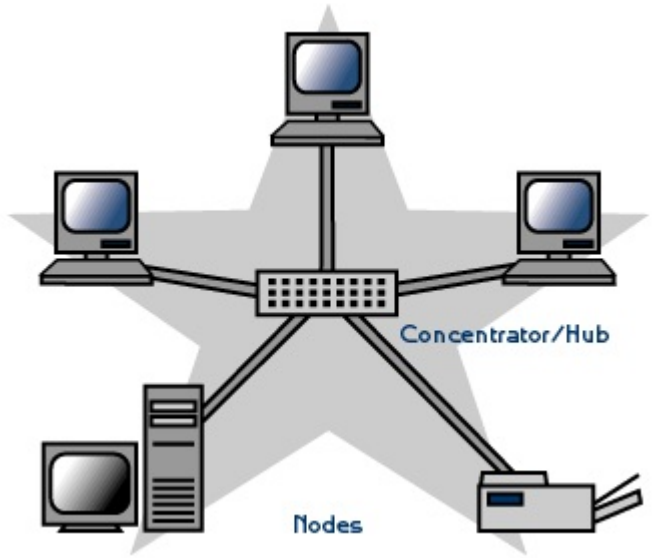
Licensed to Berend Post berend.post@it-university.nl

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



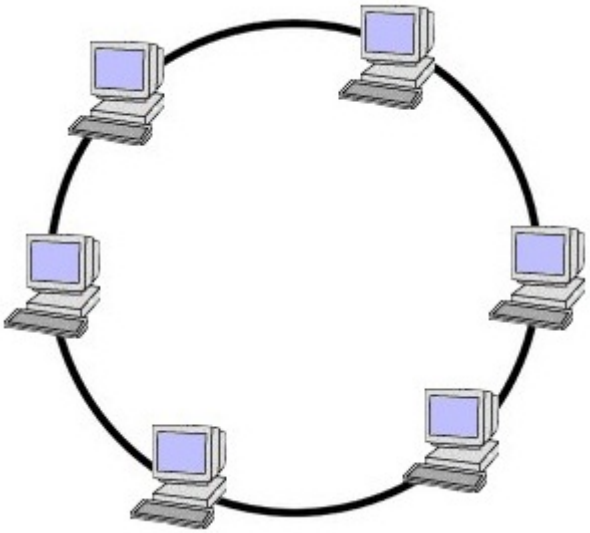
Ring

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.

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

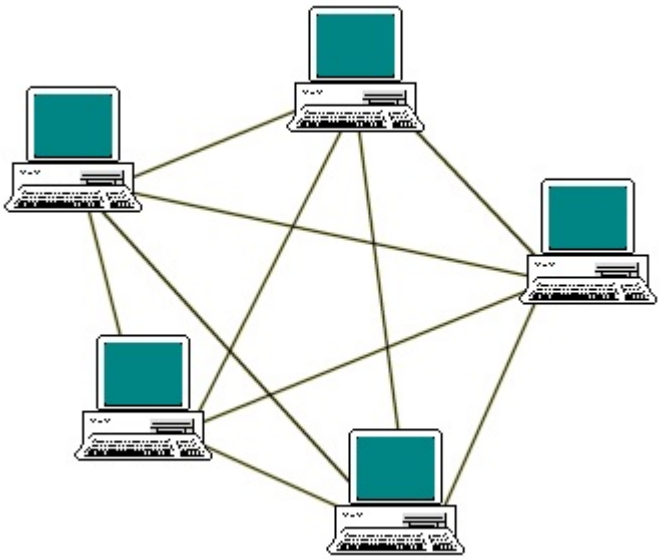


Mesh

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

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

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

Question 491

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

Question 492

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

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

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 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.

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

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 number326

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

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

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

Question 493

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 494

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

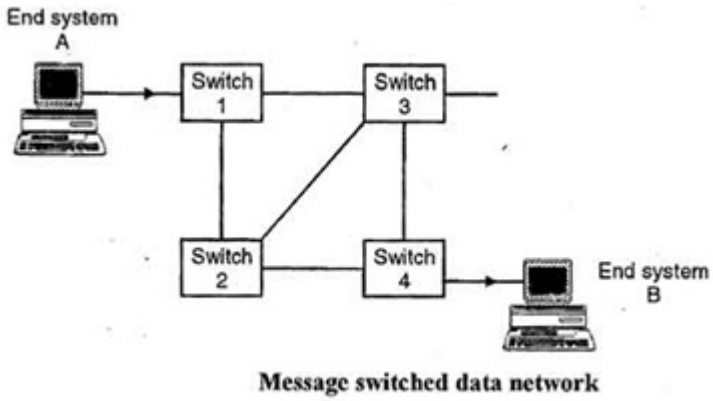
Explanation:

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



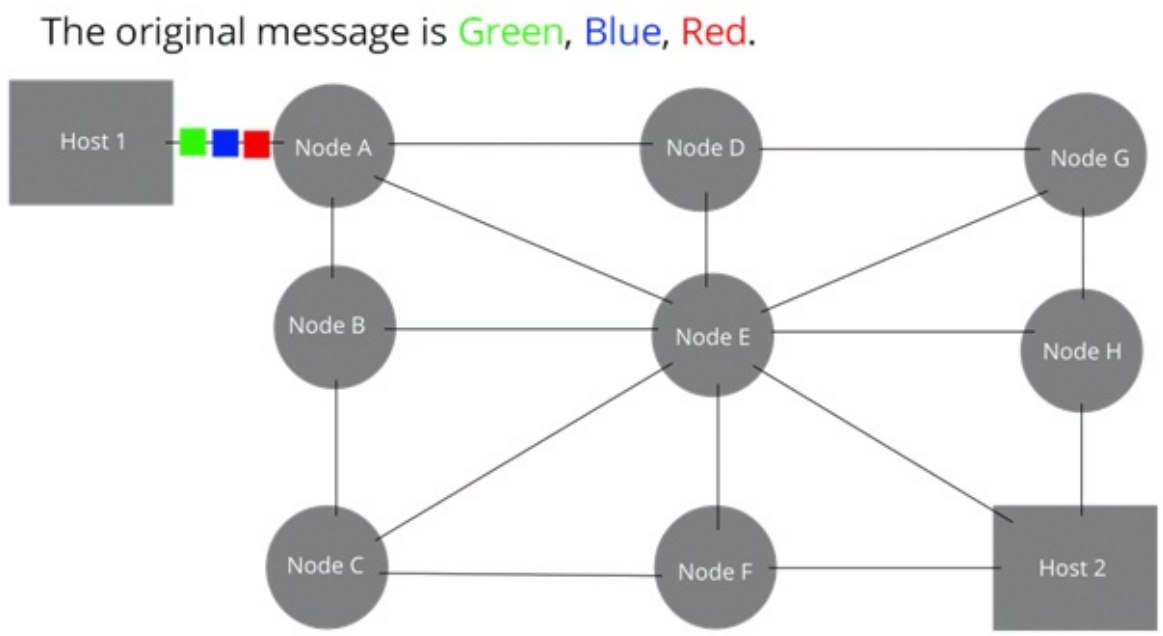
Message switched data network

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.

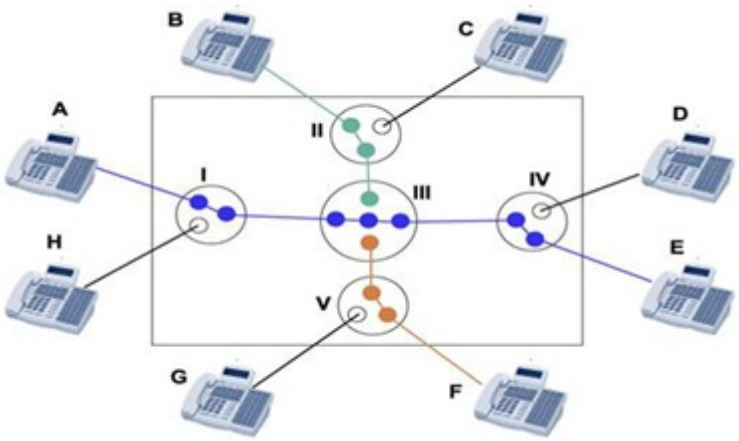
The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

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 495

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:

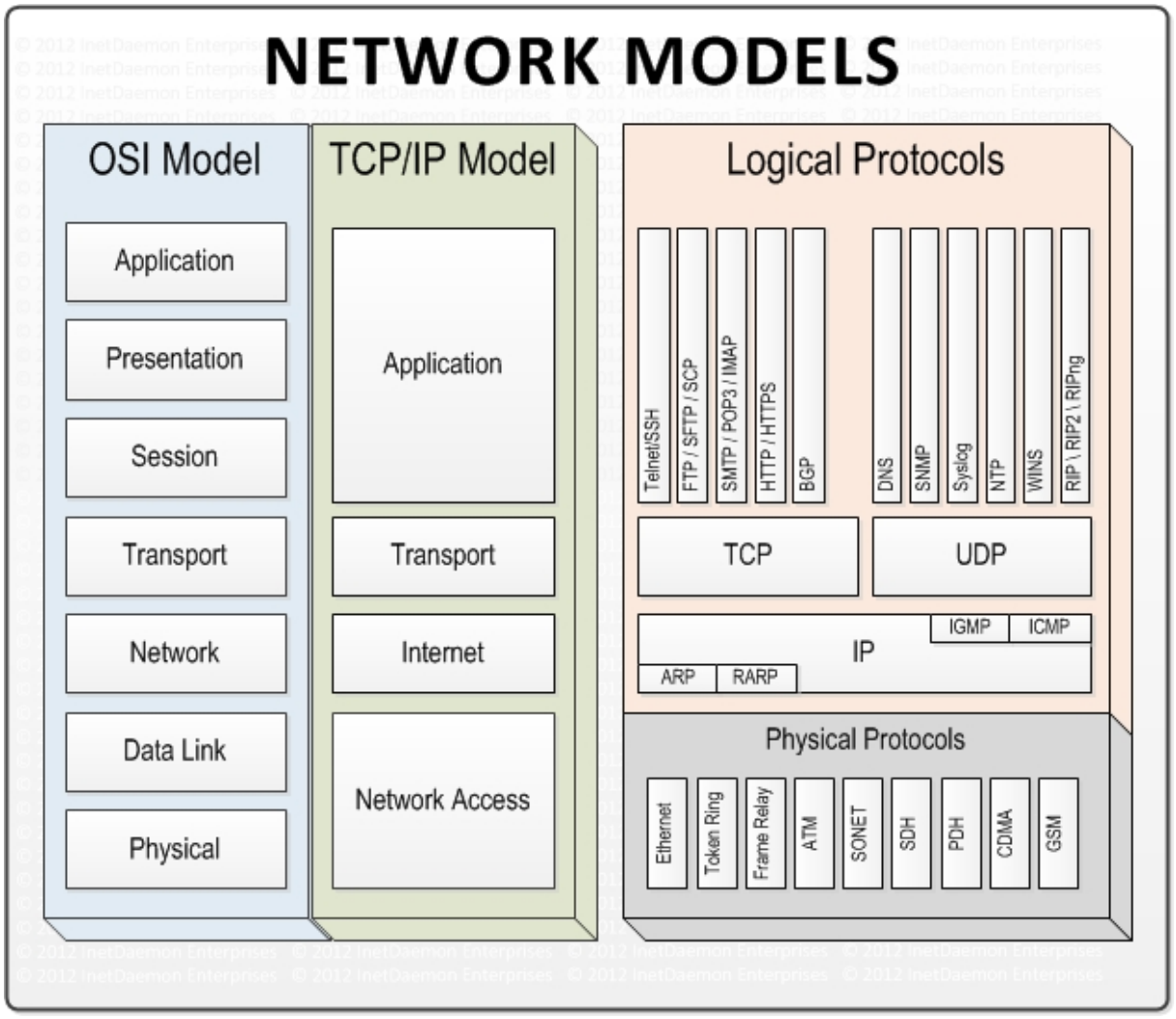
The word INCORRECTLY is the keyword used in the question. You need to find out the functionality that is not performed by LAN or WAN layer in TCP/IP model.

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.

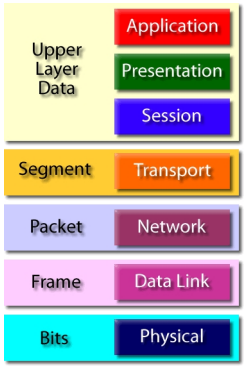
IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the 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 496

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 497

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 498

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.

Question 499

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.

For CISA exam you should know below mentioned PBS features and Risks

System Features

Description

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

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

Conferencing

Allows for conversation among several users

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

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.

Eavesdropping

No busy extension

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

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)

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

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 500

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 501

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

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

Question 502

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.

Question 503

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 504

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:

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

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 other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

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 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

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

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:

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 507

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.

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

Question 508

In a typical SDLC, which group is PRIMARILY responsible for confirming compliance with requirements?

- ☐ Steering committee
- ☐ Risk management
- ☒ Quality assurance
- ☐ Internal audit

Question 509

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 510

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.

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

Question 511

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 development procedures

Question 512

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 513

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.

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

Question 514

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 515

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 516

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 517

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:

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

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.

Question 518

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 519

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

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

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 520

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.

Question 521

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 522

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

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

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 523

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

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

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.

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 524

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

Question 525

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)

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

Question 526

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 527

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 528

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 529

An accuracy measure for a biometric system is:

- ☐ system response time.
- ☐ registration time.
- ☐ input file size.
- ☒ false-acceptance rate.

Explanation:

Explanation:

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.

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

Question 530

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 531

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.

Question 532

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

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

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.

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

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

Question 533

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 534

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

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

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.

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.

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

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.

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

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

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

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.

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

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

Question 535

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 536

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:

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

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 537

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

Question 538

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 539

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 540

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 541

Which of the following is MOST effective against system intrusions?

- ☐ Continuous monitoring
- ☒ Layered protection
- ☐ Penetration testing
- ☐ Two-factor authentication

Question 542

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 543

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.

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

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 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.

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

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.

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.

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

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

Question 544

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

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

Question 545

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 546

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 547

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.

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

Question 548

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 549

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

Question 550

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

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

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

Question 551

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 552

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.

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

Question 553

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 554

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.

Question 555

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

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

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 556

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

Question 557

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 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

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

Question 558

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 559

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 560

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.

Question 561

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.

Audit topics are supposed to be chosen based on potential for cost savings and service improvements.

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

Question 562

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 563

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:

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 564

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:

Explanation:

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

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 565

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 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 566

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 567

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 568

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 569

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.

Question 570

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.

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

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

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

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

Question 571

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 572

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 573

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 574

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:

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

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 575

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 576

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.

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

Question 577

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 578

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:

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 579

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.

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

Question 580

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 581

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.

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

Question 582

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.
- ☒ Assess whether the service provider meets the organization's data protection policies.

Question 583

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 584

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

Question 585

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.

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

Question 586

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.

Question 587

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 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.

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

Question 588

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 589

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.

Question 590

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.

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

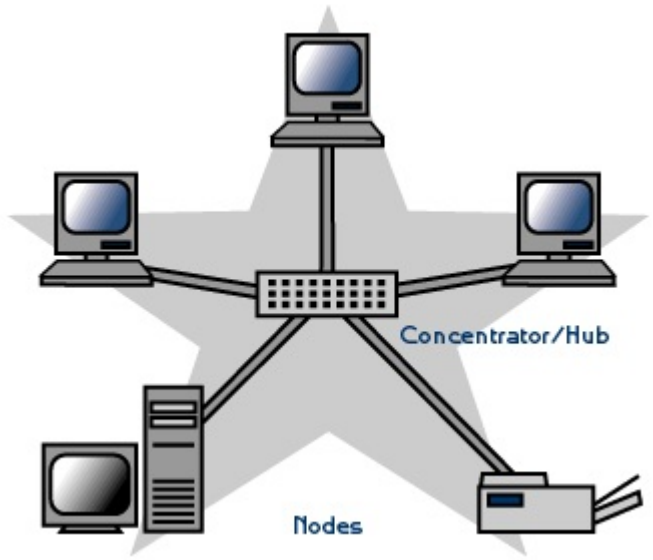
Question 591

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 592

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.

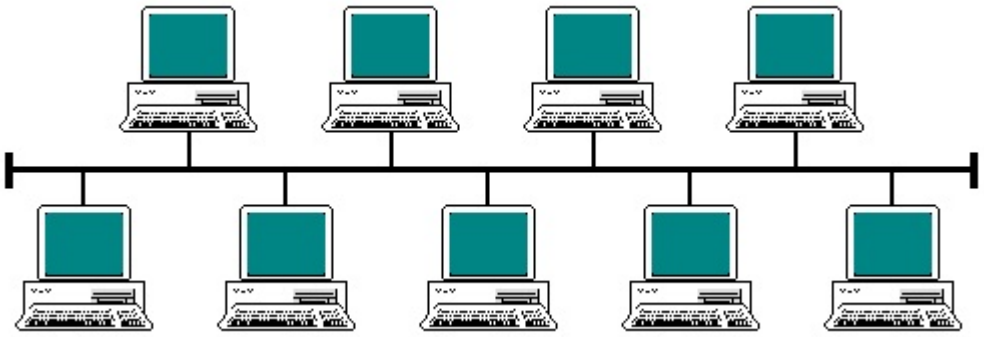
Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

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

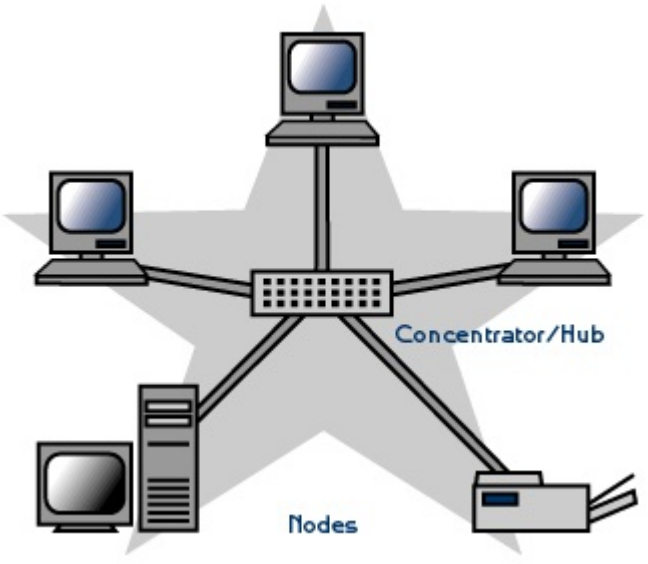
In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

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



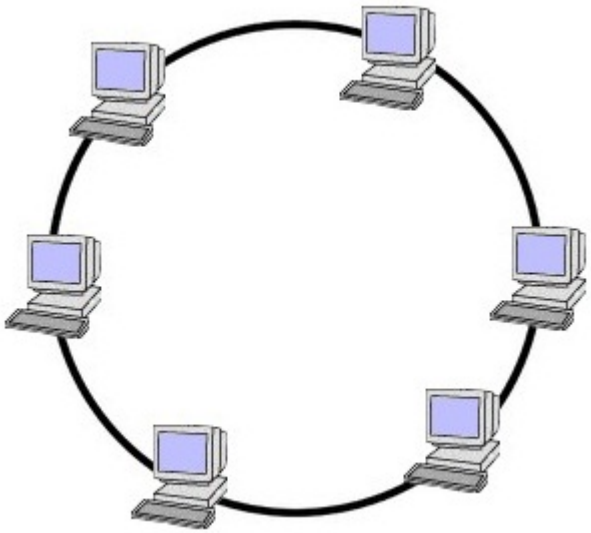
Ring

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



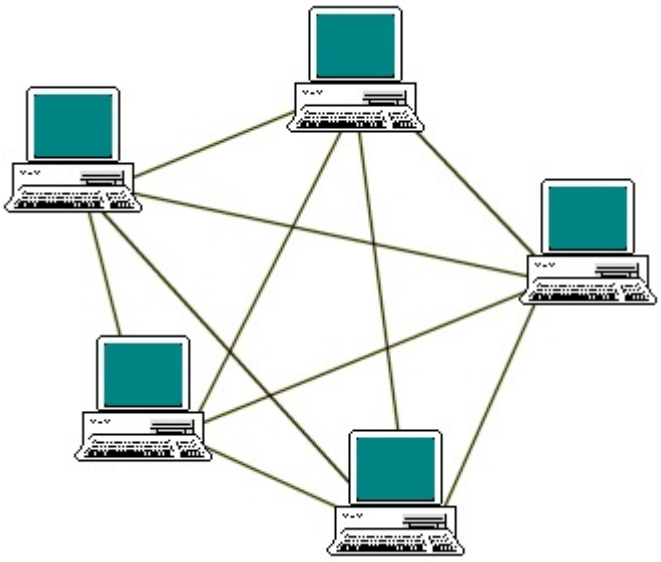
Mesh

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 593

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 594

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.

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

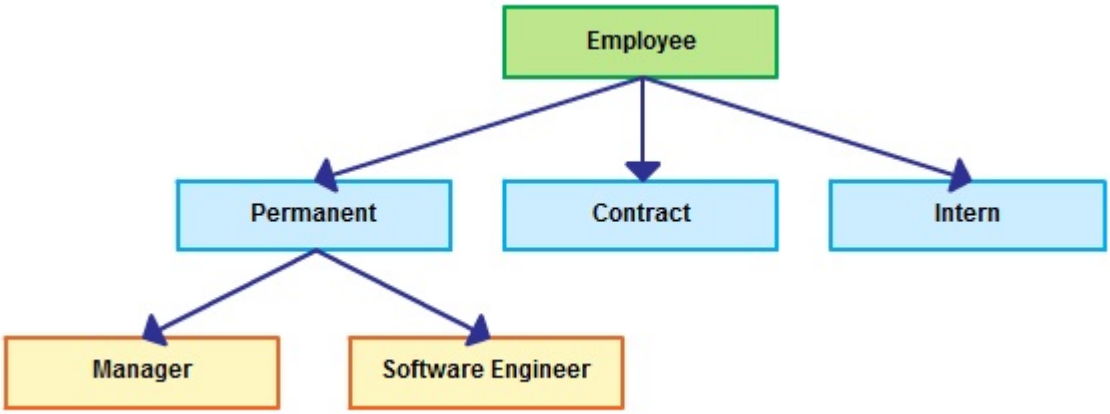
Licensed to Berend Post berend.post@it-university.nl

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



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.

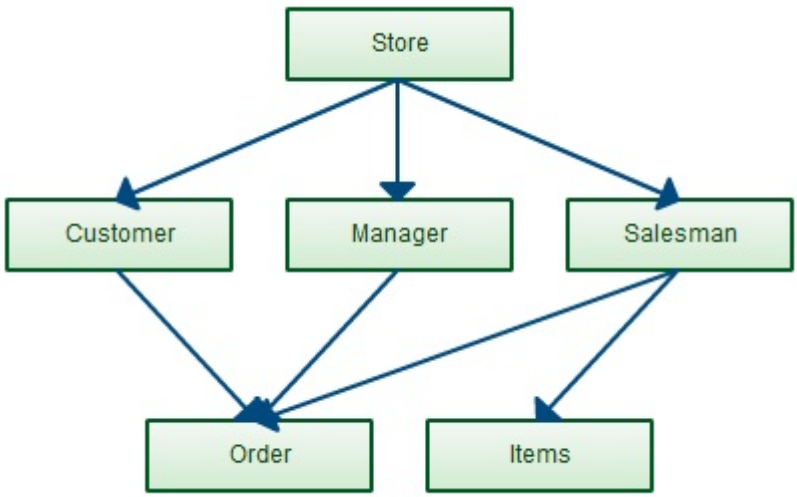
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between records: one owner, many members. A record may be an owner in any number of sets, and a member in any number of sets.

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

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



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.

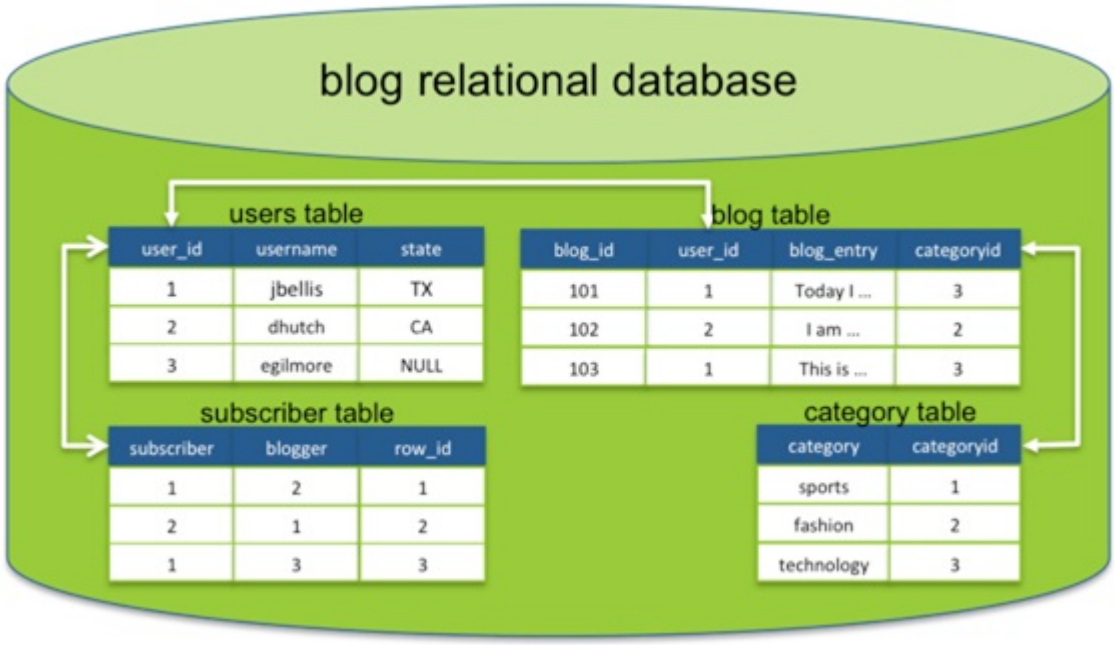
In the relational model, related records are linked together with a "key".

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.

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

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



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:

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

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 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 595

Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

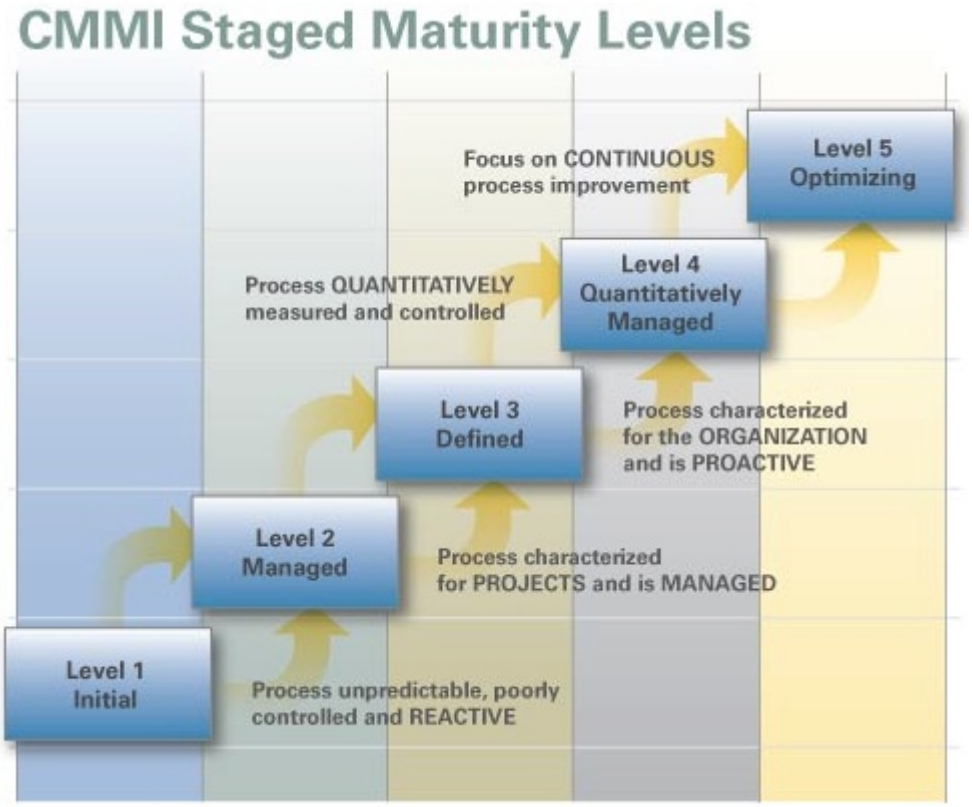
- ☒ Initial, Managed, Defined, Quantitatively managed, optimized
- ☐ Initial, Managed, Defined, optimized, Quantitatively managed
- ☐ Initial, Defined, Managed, Quantitatively managed, optimized
- ☐ Initial, Managed, Quantitatively managed, Defined, optimized

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.

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

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.

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)

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

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.

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

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

CISSP Official study guide page number 693

Question 596

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 597

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 598

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:

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

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 599

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, 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:

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 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 600

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 601

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.

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

Question 602

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

Question 603

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

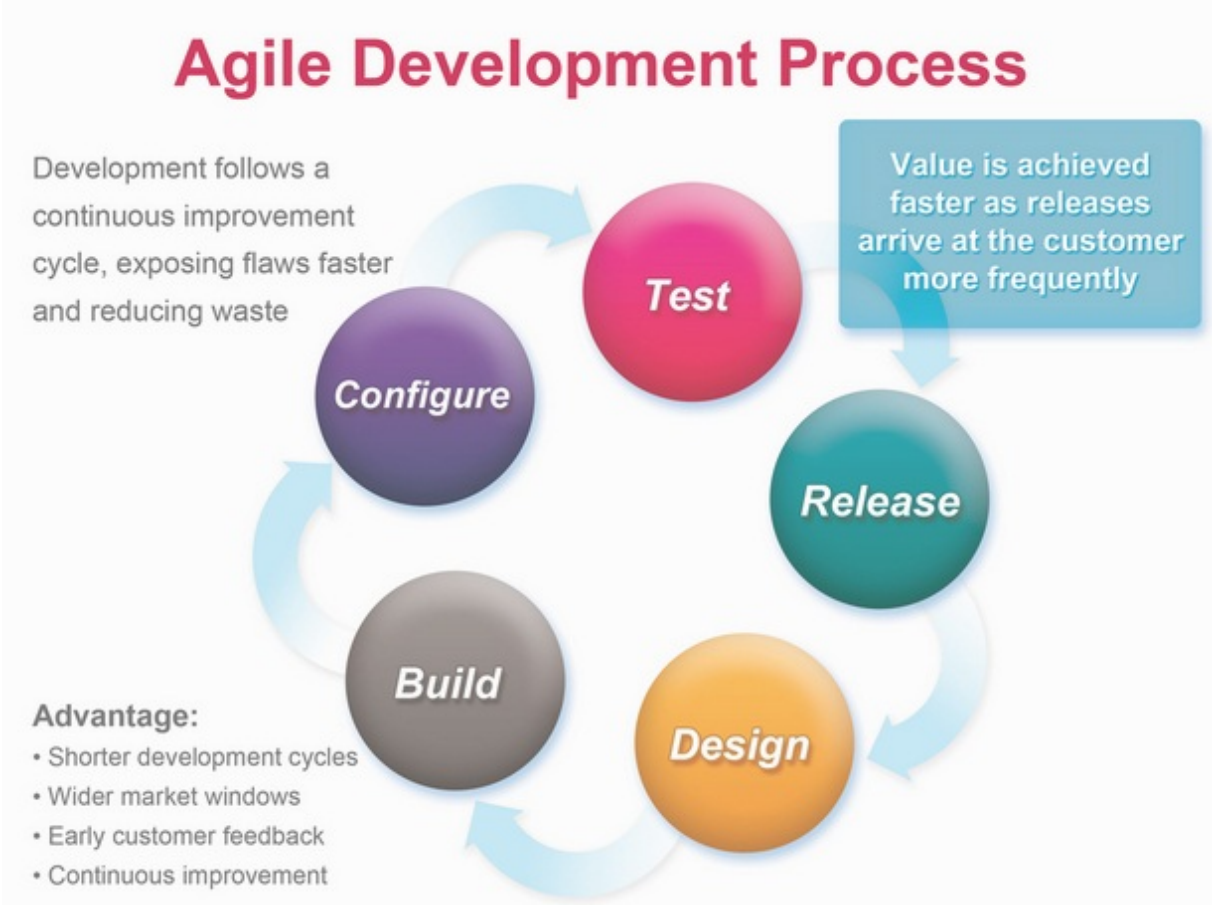
Explanation:

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 604

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 605

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 606

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

Question 607

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:

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

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 608

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 609

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 610

Which of the following are BEST suited for continuous auditing?

- ☐ Manual transactions
- ☐ Irregular transactions
- ☐ Low-value transactions
- ☒ Real-time transactions

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

Question 611

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 612

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 613

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 614

_____ (fill in the blank) 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:

Control totals should be implemented as early as data preparation to support data integrity at the earliest point possible.

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

Question 615

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:

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 616

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.

Question 617

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

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

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 618

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:

Access control software is an active control designed to prevent unauthorized access to data.

Question 619

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:

System Features

Description

Risk

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

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

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

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 620

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 621

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 622

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 623

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 624

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 625

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:

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 626

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

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

Question 627

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:

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 628

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 629

Which of the following is the GREATEST risk of cloud computing?

- ☐ Reduced performance
- ☒ Disclosure of data
- ☐ Lack of scalability
- ☐ Inflexibility

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

Question 630

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 631

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.

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 632

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

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

Question 633

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 634

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 635

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.

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

Question 636

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 637

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 638

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

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

Question 639

A design company has multiple name and address file 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 640

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 641

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

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

Question 642

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 643

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.

Question 644

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.

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

Question 645

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 646

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 647

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.

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

Question 648

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 649

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 650

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.

Question 651

Who is responsible for restricting and monitoring access of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☒ Security Administrator

Explanation:

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

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

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

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

Question 652

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.

Question 653

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 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.

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

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

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.

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

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.

The following answers are incorrect:

The other types of computers are not example of diskless workstation.

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 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 654

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

Question 655

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.

Question 656

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.

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

Question 657

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.

Question 658

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 659

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.

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

Question 660

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 661

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 662

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

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

Question 663

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.

Question 664

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.

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

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

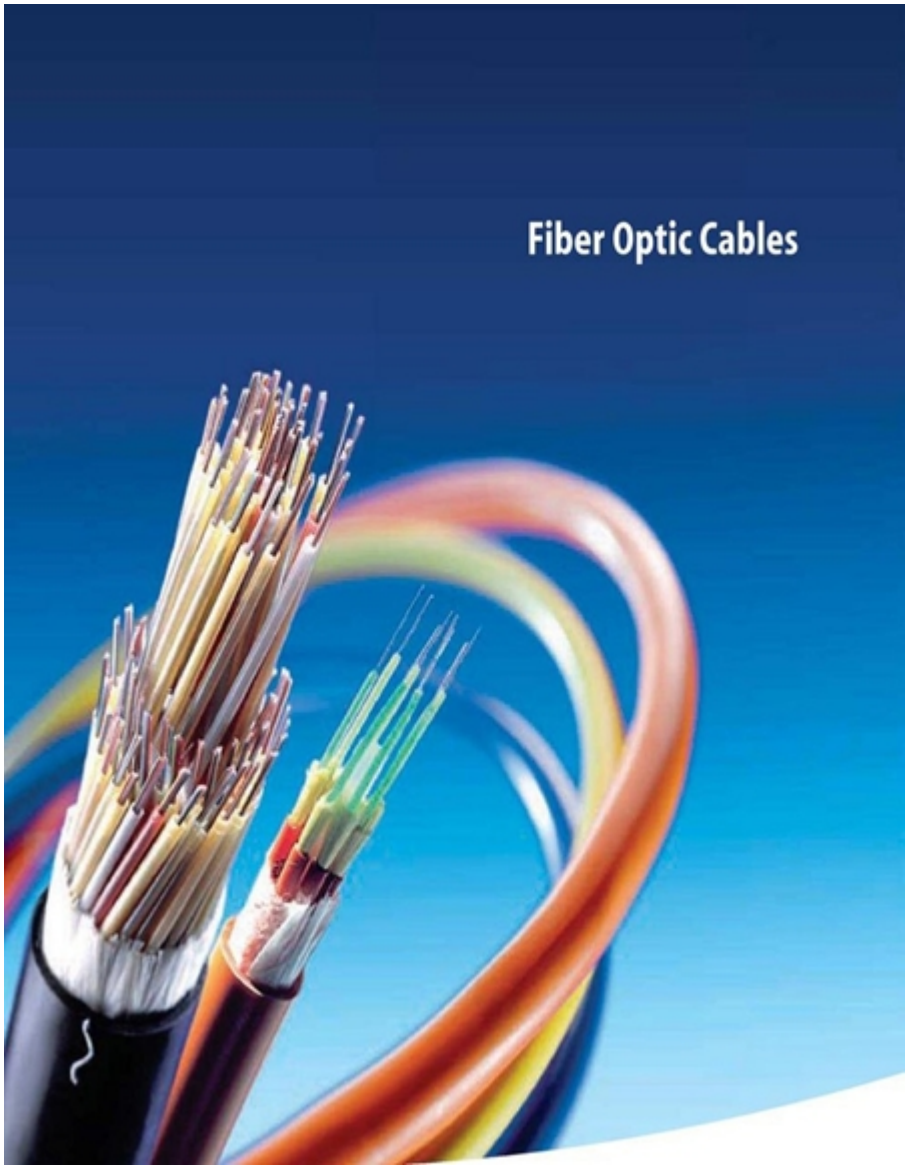
Licensed to Berend Post berend.post@it-university.nl

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.

Fiber Optics



Microwave radio system

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

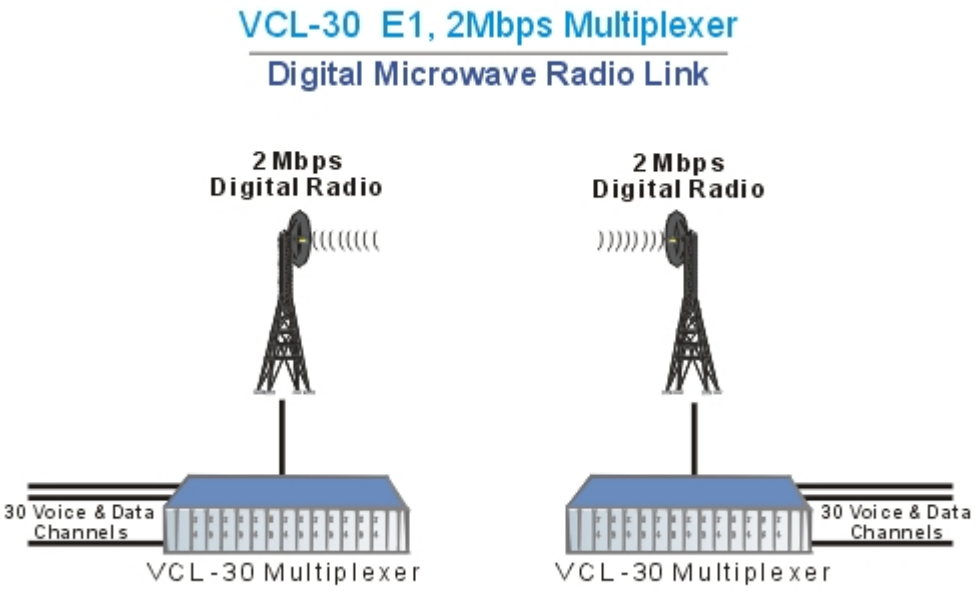
Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

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 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.

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

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 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 665

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

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

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.

Question 666

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 667

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 668

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.

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

Question 669

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 670

In an organization that has a staff-rotation policy, the MOST appropriate access control model is:

- ☒ role based.
- ☐ discretionary.
- ☐ mandatory.
- ☐ lattice based.

Question 671

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 672

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.

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

Question 673

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 674

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 675

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

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

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 676

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 677

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.

Question 678

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 679

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 680

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 681

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

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:

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.

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

CISA review manual 2014 Page number 188

Question 682

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.

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

Question 683

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 684

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 685

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:

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

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.

Question 686

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 687

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 688

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

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

Question 689

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 690

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. 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 691

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 692

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 693

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 694

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 695

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 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:

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

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

Question 696

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 697

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

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

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.

Question 698

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 699

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 700

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.

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

However, a virtual private network (VPN) would offer a more secure means of enabling this access 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 701

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 702

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 703

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 704

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.

Question 705

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

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

(piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

Question 706

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 707

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

Question 708

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 709

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

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

Question 710

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 711

An existing system is being replaced with a new application package. User acceptance testing should ensure that:

- ☐ data from the old system has been converted correctly
- ☒ the new system functions as expected
- ☐ the new system is better that the old system
- ☐ there is a business need for the new system

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

Question 712

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 713

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 714

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:

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

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 715

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 716

In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

- ☐ Reporting
- ☐ Attacks
- ☒ Discovery
- ☐ Planning

Question 717

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 718

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 719

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 720

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 721

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 722

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.

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

Question 723

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 724

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 725

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.

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

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:

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 726

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 727

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 728

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 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.

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

Question 729

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

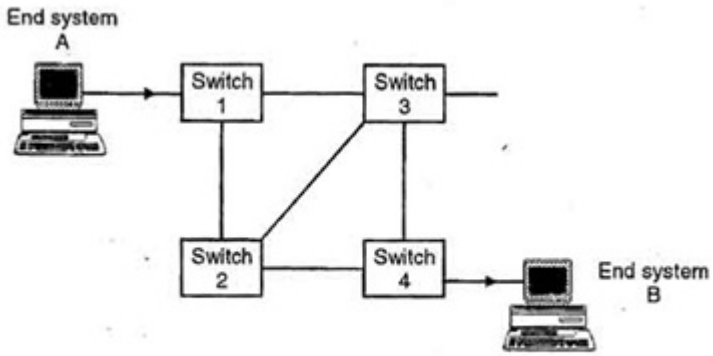
Explanation:

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 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



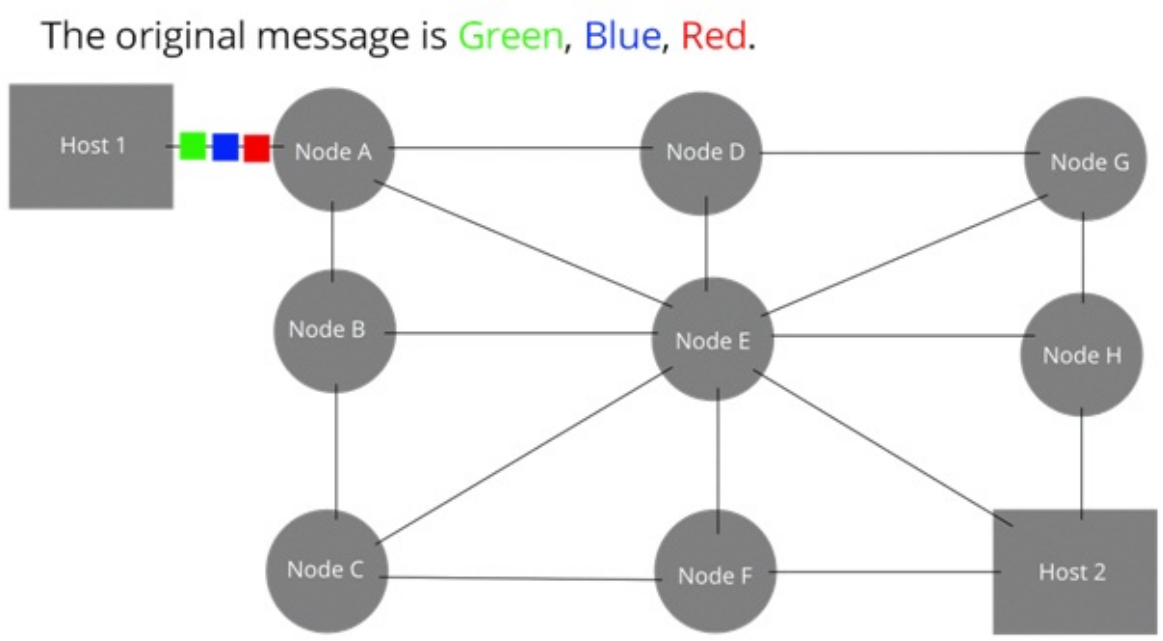
Message switched data network

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.

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

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.

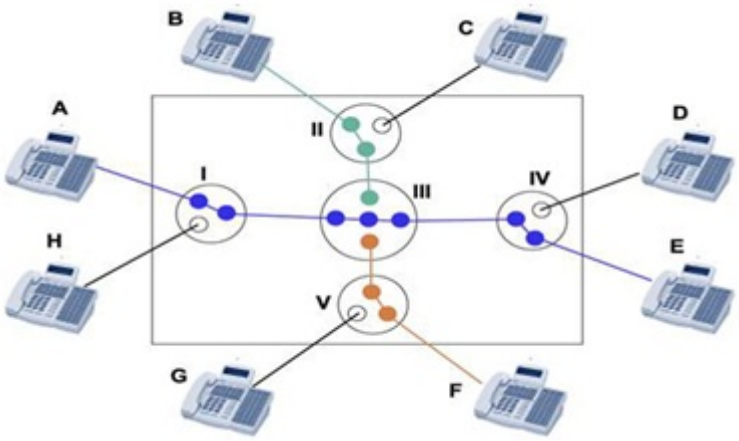
The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

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.

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.

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,

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

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 730

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 731

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.

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

Question 732

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 733

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 734

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.

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

Question 735

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:

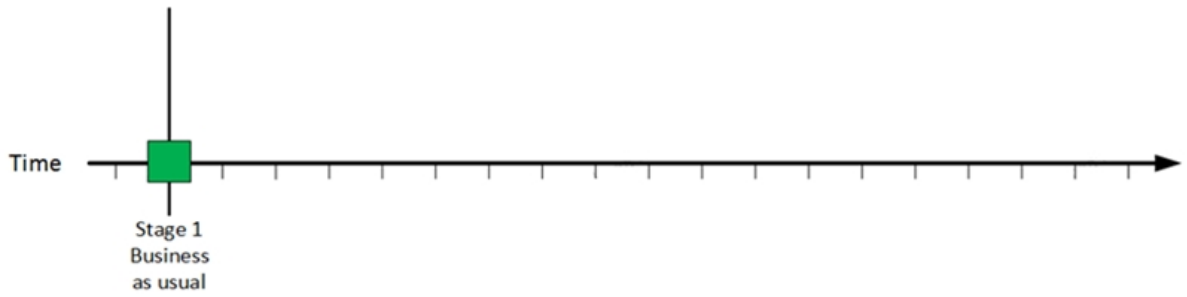
Explanation:

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

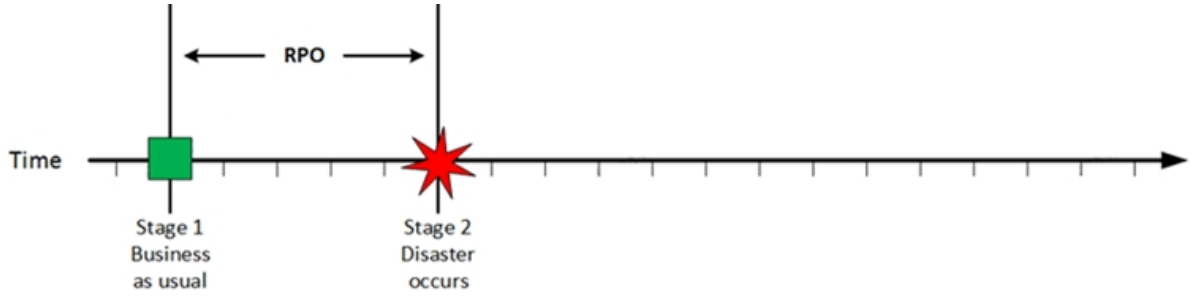


At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

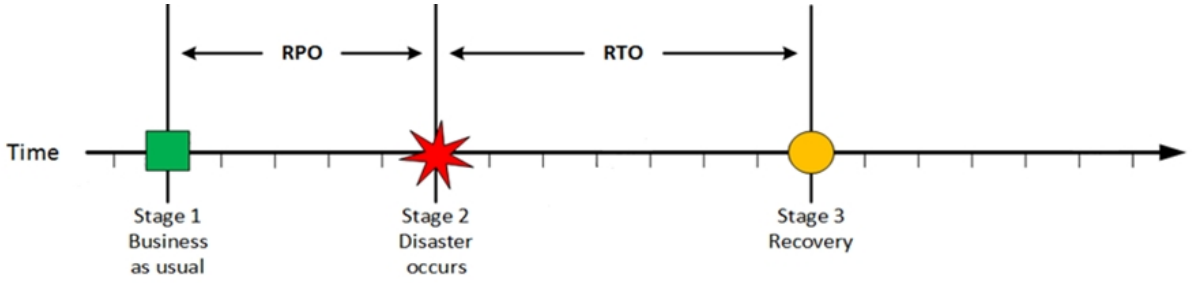
Licensed to Berend Post berend.post@it-university.nl



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

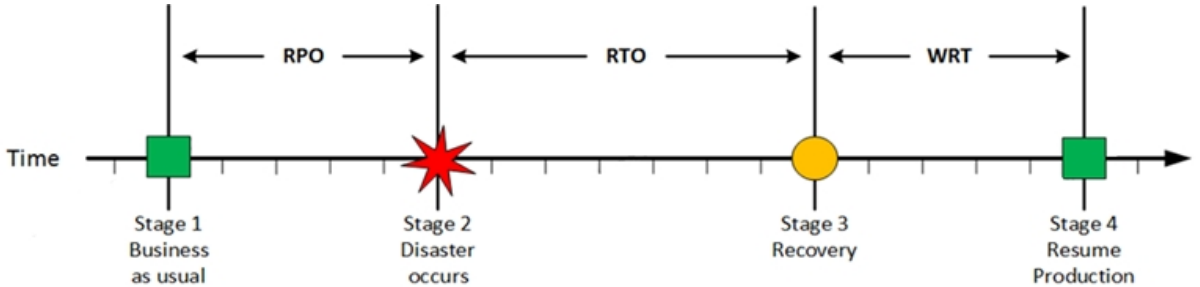
Recovery



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

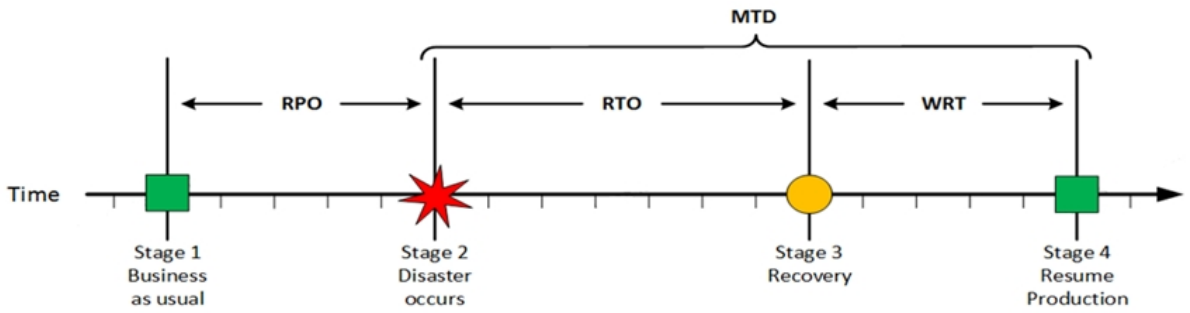
Resume Production



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.

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.

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 736

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 737

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 738

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

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

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 739

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 740

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 741

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.

Question 742

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

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

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.

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 743

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 744

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 745

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

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

Question 746

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 747

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 748

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 749

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 750

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 751

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.

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

Question 752

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 753

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).

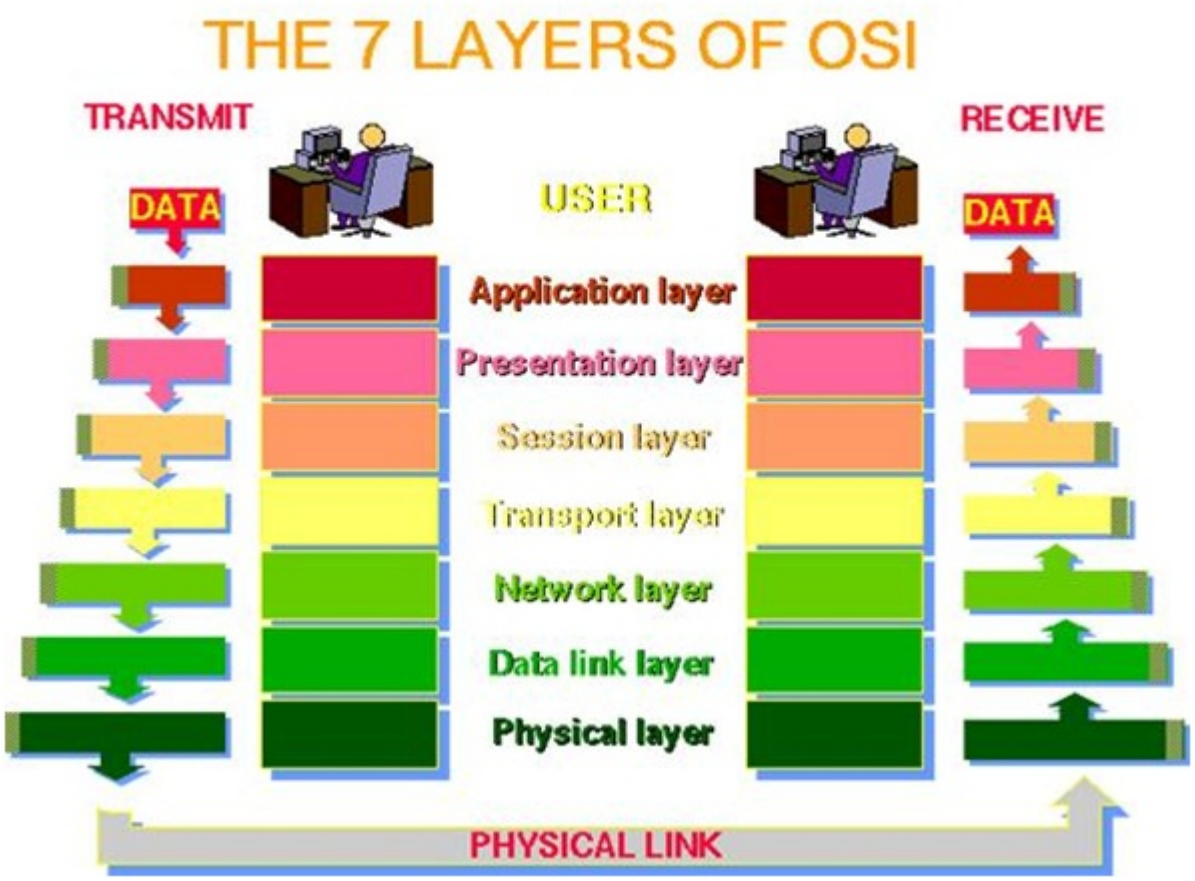
For your exam you should know below information about OSI model:

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

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



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:

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

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:

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.

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

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.

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.

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

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

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:

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

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.

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 754

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:

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

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 755

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 756

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 757

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:

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

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 758

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.

Question 759

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 760

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 761

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 762

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 763

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 764

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 765

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):

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.

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

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:

CISA review manual 2014 page number 275

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

Question 766

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 767

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 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 768

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.

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

Question 769

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 770

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.

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

Question 771

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, 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 772

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 773

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

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

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 774

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 775

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 776

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.

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

Question 777

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 778

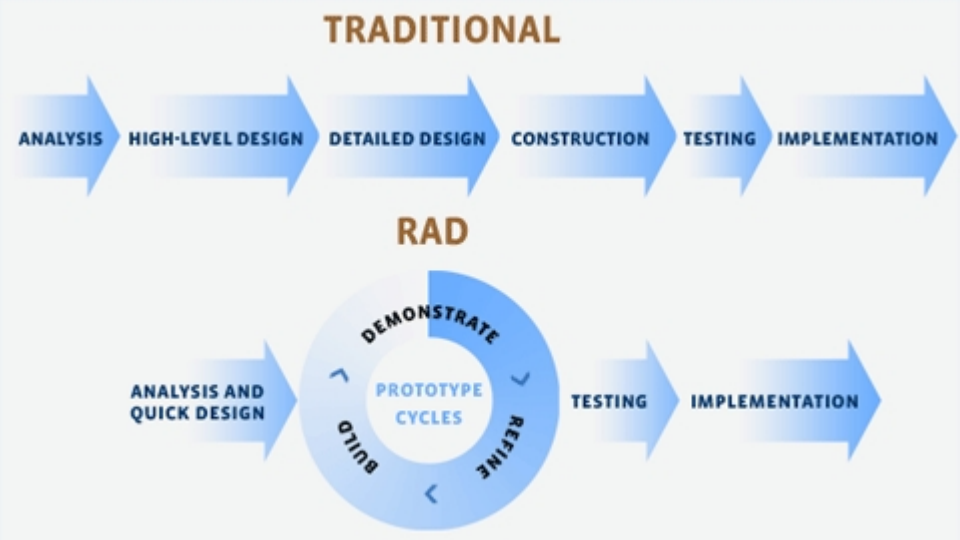
Which of the following software development methodology uses minimal planning and in favor of rapid prototyping?

- ☐ 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 779

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

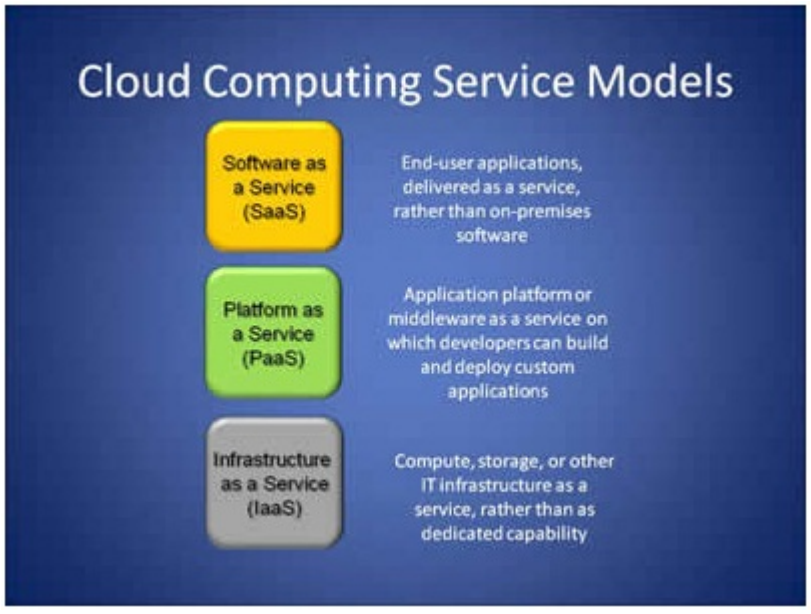
Explanation:

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:

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.

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.

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

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.

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:

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

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.

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 780

isk 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.

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

Question 781

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 782

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 783

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 784

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.

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

Question 785

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 786

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.

Question 787

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:

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

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 788

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 789

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 790

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:

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

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.

Question 791

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 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 792

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.

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

Question 793

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?

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

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 794

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:

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.

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

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 795

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.

Question 796

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.

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

Question 797

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 798

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

Question 799

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 800

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

Question 801

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 802

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:

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.

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

Question 803

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 804

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 805

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

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

Question 806

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.

Question 807

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 808

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

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

Question 809

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 810

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 811

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 hardware needs are not as critical as allocating resources during short-term planning for the IS department.

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

Question 812

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 813

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

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.

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

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 814

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

Question 815

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

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

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

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.

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

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 816

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 817

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 818

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 819

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 820

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 821

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:

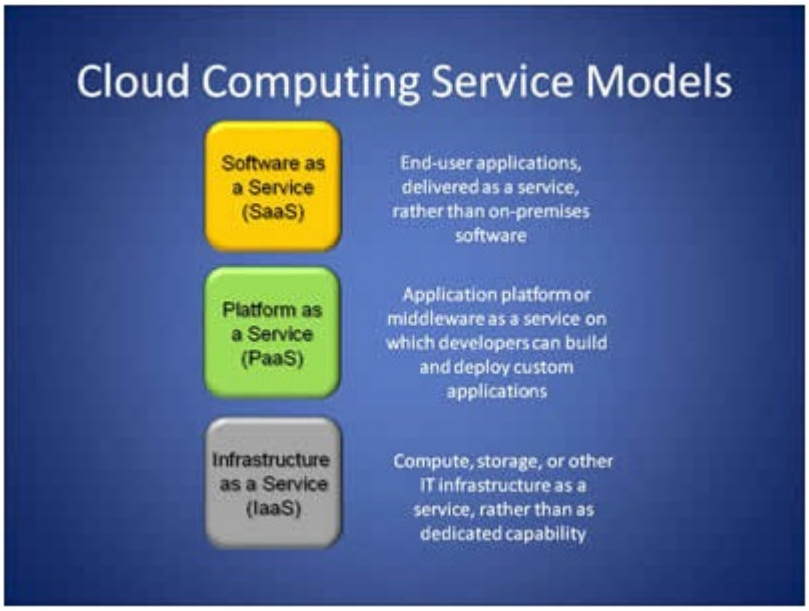
Licensed to Berend Post berend.post@it-university.nl

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



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.

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

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 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.

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

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.

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

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

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 822

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 823

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.

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:

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

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 824

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

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

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.

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.

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

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.

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.

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

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.

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

CISA review manual 2014 Page number 188

Question 825

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 826

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:

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

Explanation:

To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

Question 827

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 828

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 829

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:

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

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.

Question 830

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:

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 831

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 832

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.

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.

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

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:

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.

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 314

Official ISC2 guide to CISSP CBK 3rd Edition Page number 350

Question 833

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 834

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

Question 835

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:

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

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.

Question 836

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 837

Two-factor authentication can be circumvented through which of the following attacks?

- ☐ Denial-of-service
- ☒ Man-in-the-middle
- ☐ Key logging
- ☐ Brute force

Explanation:

Explanation:

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

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 838

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:

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 839

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 840

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.

Question 841

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 842

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.

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

Question 843

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 844

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 845

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

Question 846

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:

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

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 847

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:

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

CISA review manual 2014 Page number 348

Question 848

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.

Question 849

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 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.

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

Question 850

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 851

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 852

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 853

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 854

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

Question 855

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 856

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:

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

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

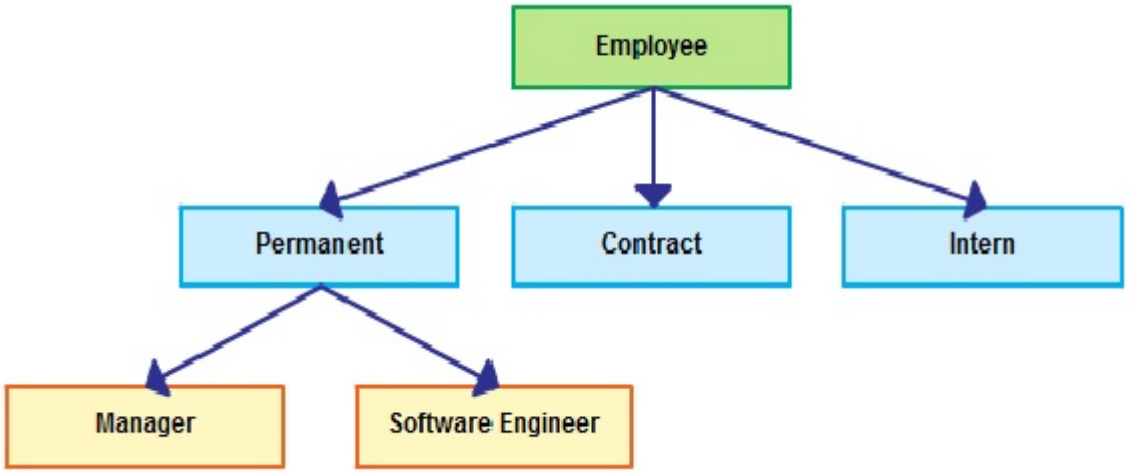
Hierarchical database model

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.

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.

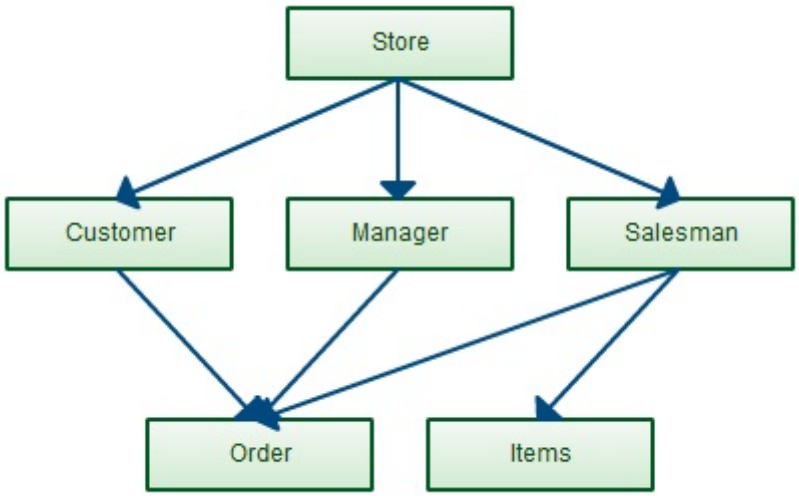
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between 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.

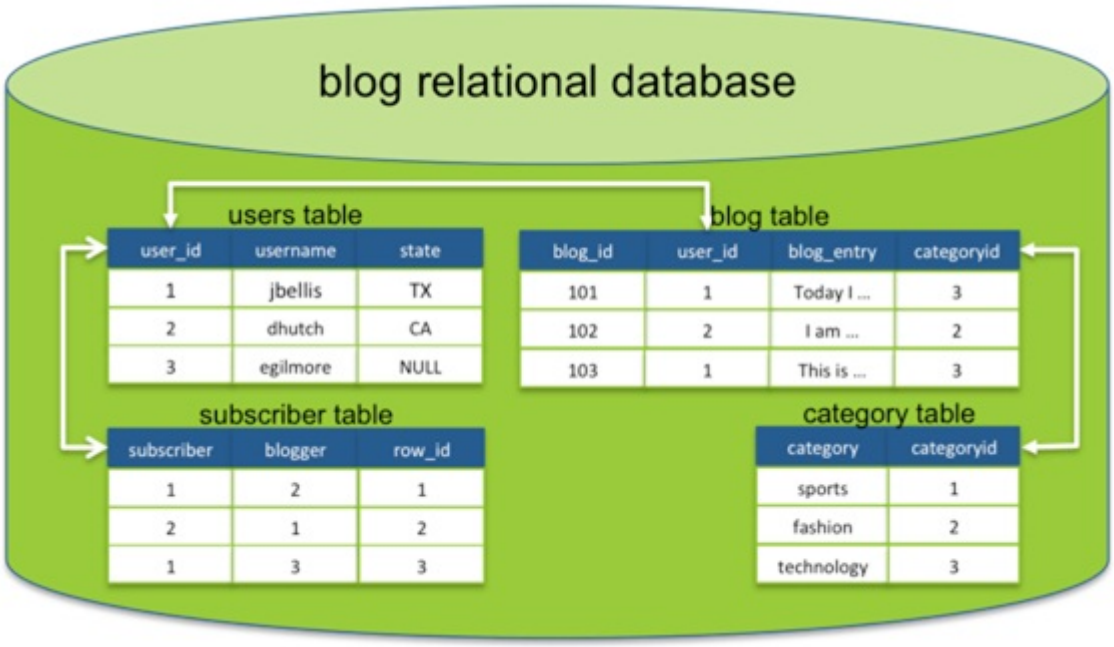
In the relational model, related records are linked together with a "key".

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:

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 857

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 858

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.

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

Question 859

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 860

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.

Question 861

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.

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

Question 862

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.

Question 863

Which of the following is the MOST important reason for logging firewall activity?

- ☐ Intrusion detection
- ☒ Auditing purposes
- ☐ Firewall tuning
- ☐ Incident investigation

Question 864

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 865

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 866

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 867

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 868

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:

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

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.

Question 869

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 870

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 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.

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

Question 871

Which of the following would be 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 872

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 873

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

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

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.

Question 874

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 875

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 876

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 877

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 878

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.

Question 879

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

Question 880

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.

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

Question 881

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.

Question 882

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 883

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.

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

Question 884

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 885

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 886

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

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

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.

Question 887

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 888

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 889

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 890

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 891

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

Question 892

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.

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

Question 893

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 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 894

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.

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

Question 895

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 896

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 897

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.

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

Question 898

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 899

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 900

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

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

Question 901

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 902

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 903

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:

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

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.

Question 904

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.

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 905

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,

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

but not a server failure. Choice D provides an alternative power source in the event of an energy failure.

Question 906

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

Question 907

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan 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

Question 908

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.

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

Question 909

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 910

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

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

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

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.

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.

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 354 and 355

Question 911

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 912

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 913

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 914

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 915

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.

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

Question 916

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.

Question 917

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.

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

Question 918

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 919

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.

Question 920

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

Question 921

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

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

Question 922

Which of the following is the MOST critical characteristic of a biometric system?

- ☐ Registration time
- ☐ Throughput rate
- ☒ Accuracy
- ☐ Ease of use

Question 923

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:

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 924

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 925

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:

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

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 926

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

Question 927

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 928

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 929

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.

Question 930

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 931

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:

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

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 932

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 933

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.

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

Question 934

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.

Question 935

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 936

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 937

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 938

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 939

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.

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

Question 940

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 941

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 942

Which of the following is the MOST important feature of access control software?

- ☒ Authentication
- ☐ Violation reporting
- ☐ Nonrepudiation
- ☐ Identification

Question 943

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

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

Question 944

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 945

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.

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

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

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

Question 946

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.

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

Question 947

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 948

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.

Question 949

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

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

Question 950

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

Question 951

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 952

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.

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

Question 953

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.

Question 954

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 955

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 956

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 957

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.

Question 958

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.

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

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:

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

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

Question 959

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 960

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 961

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.

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

Question 962

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 963

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 964

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

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

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 965

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 966

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:

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.

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

Question 967

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:

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 968

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 969

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

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

business processes. Identification of resources for business resumption will occur after the tasks mentioned.

Question 970

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

Question 971

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 972

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 973

Which of the following is a MAJOR benefit of using a wireless network?

- ☐ Faster network speed
- ☒ Stronger authentication
- ☐ Protection against eavesdropping
- ☐ Lower installation cost

Question 974

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.

Question 975

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:

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

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

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 976

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 are good practices, but they do not directly prevent the loss of data Integrity and confidentiality during communication through a network.

Question 977

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

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

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.

Question 978

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 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.

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

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 979

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:

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).

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 980

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.

Question 981

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.

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

Question 982

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

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.

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

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

Question 983

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 984

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 985

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 986

Which of the following would provide 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 987

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 988

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:

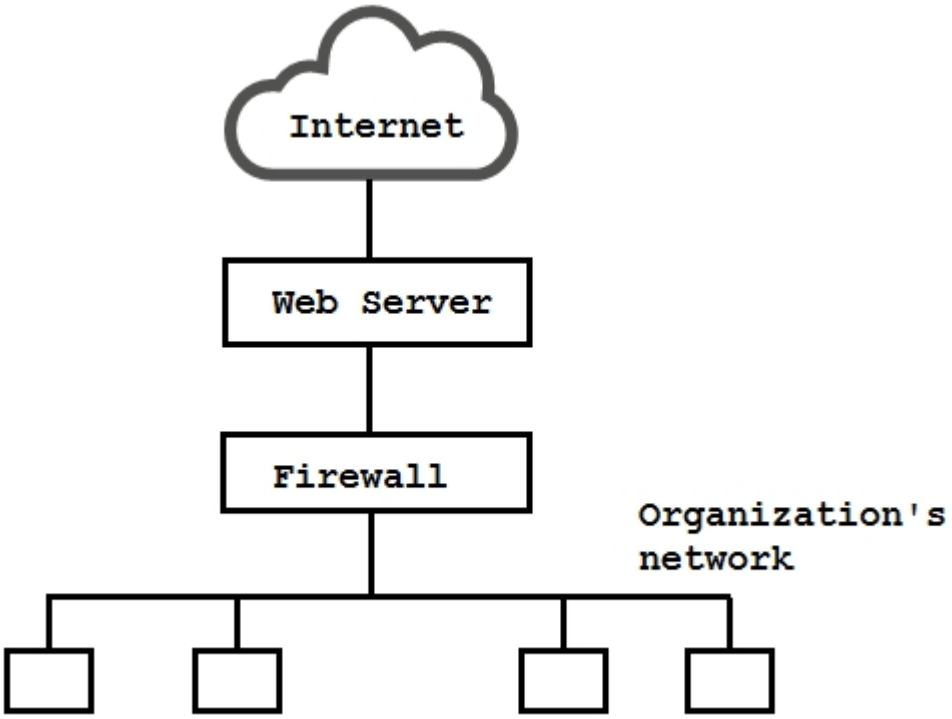
Explanation:

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.

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

Question 989

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:

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.

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

Question 990

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.

Question 991

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 992

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

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

Explanation:

Explanation:

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.

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

Question 993

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 994

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.

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:

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

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 995

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:

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

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

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 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.

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

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 996

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 997

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 998

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 999

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 1000

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.

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

Question 1001

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.

Question 1002

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

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

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.

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.

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

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.

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 1003

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 1004

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

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

Question 1005

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 1006

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 1007

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

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

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.

Question 1008

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 1009

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.

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

Question 1010

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.

Question 1011

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.

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

Question 1012

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 1013

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.

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

Question 1014

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 1015

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.

Question 1016

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.

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.

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

Question 1017

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.

Question 1018

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 planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

Question 1019

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.

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

Question 1020

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.

Question 1021

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.

Question 1022

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

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

Question 1023

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:

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 1024

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 1025

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 1026

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:

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

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 1027

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:

Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

Question 1028

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 1029

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

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

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 1030

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.

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:

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 1031

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 1032

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 1033

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 1034

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 1035

Which of the following provides for the GREATEST cost reduction in a large data center?

- ☒ Server consolidation
- ☐ Staff rotation
- ☐ Power conditioning
- ☐ Job-scheduling software

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

Question 1036

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.

Question 1037

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.

Question 1038

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:

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

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 1039

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.

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

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

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

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

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.

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

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

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

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 1040

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):

 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

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:

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

CISA review manual 2014 page number 275

Question 1041

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 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:

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

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.

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 1042

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 1043

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.

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

Question 1044

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.

Question 1045

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

Question 1046

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,

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

and covert listening devices. The attacker can also easily download large quantities of data onto backup media or portable devices.

Question 1047

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 1048

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.

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

Question 1049

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 1050

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 1051

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 1052

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 1053

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 1054

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

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

Question 1055

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.

Question 1056

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

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.

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 1057

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- ☒ True
- ☐ False

Explanation:

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

Explanation:

Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

Question 1058

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 1059

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.

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

Question 1060

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 1061

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

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

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.

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

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

Question 1062

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.

Question 1063

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.

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

Question 1064

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 1065

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:

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 1066

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.

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

Question 1067

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 1068

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 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

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

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.

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

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

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

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

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

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

http://pakaccountants.com/what-is-control-risk/

http://accounting-simplified.com/audit/risk-assessment/audit-risk.html

Question 1069

Which type of risk would MOST influence the selection of a sampling methodology?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☒ Detection

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

Question 1070

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 1071

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 1072

Which of the following activities would be 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.

Question 1073

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 1074

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 1075

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 1076

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 1077

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 1078

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

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

Question 1079

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.

Question 1080

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 1081

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.

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

Question 1082

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 1083

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.

Question 1084

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 1085

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:

Point-to-point protocol

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

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

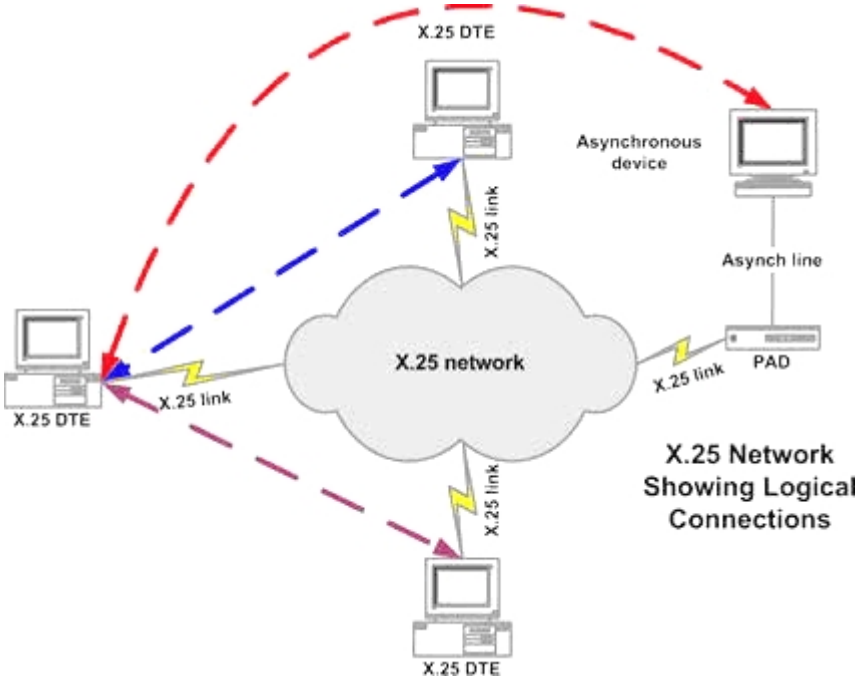
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

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

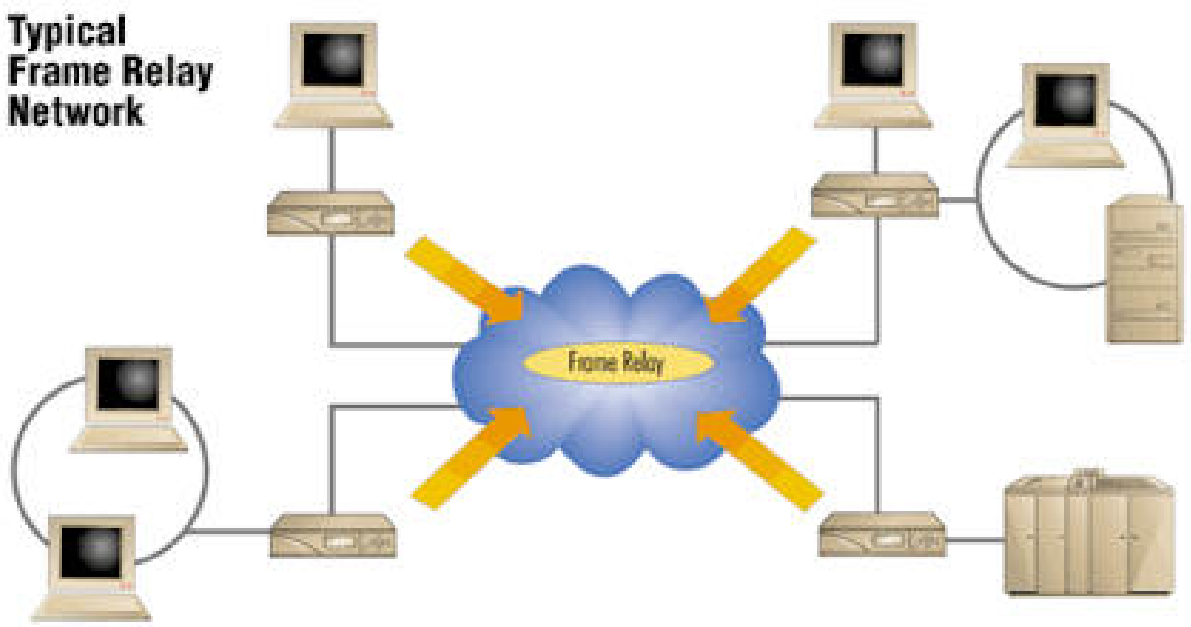
Two main types of equipment's are used in Frame Relay

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



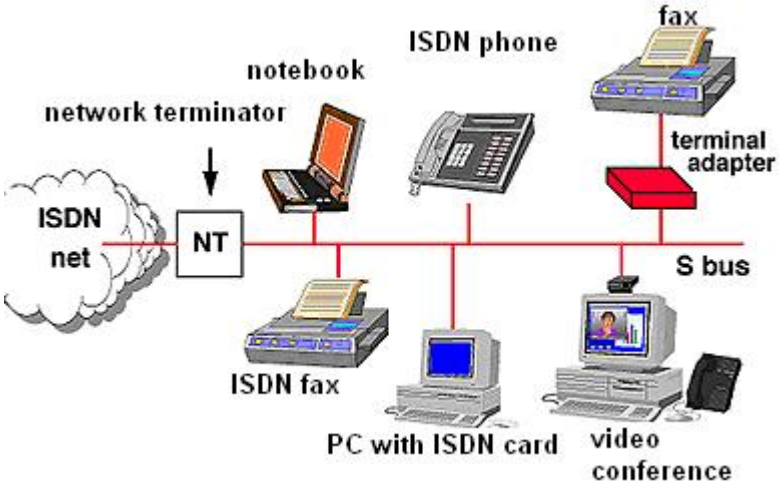
Frame Relay

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

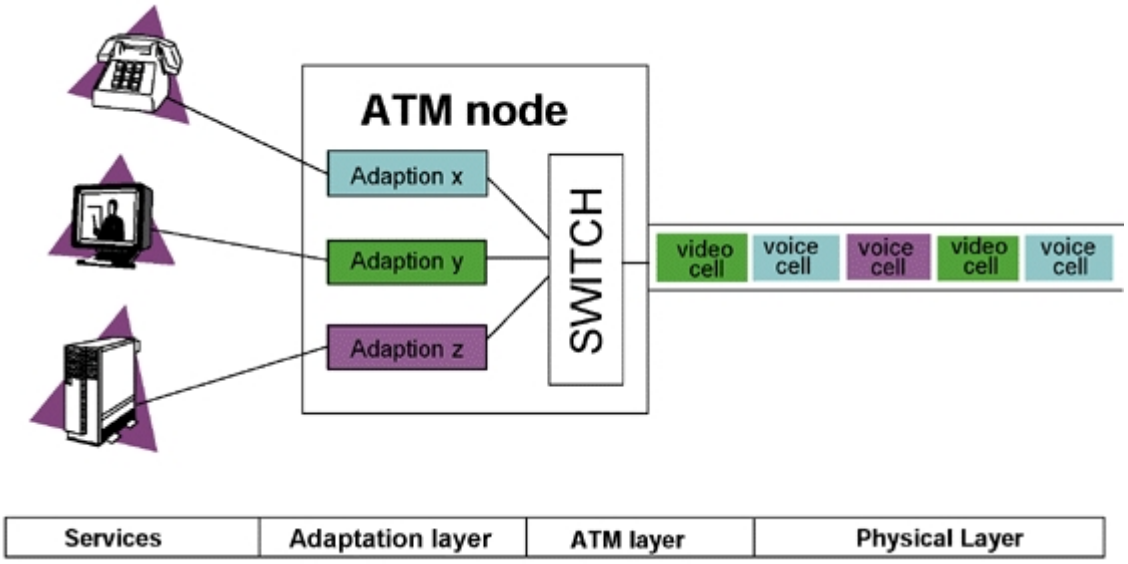
Uses Cell switching method

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



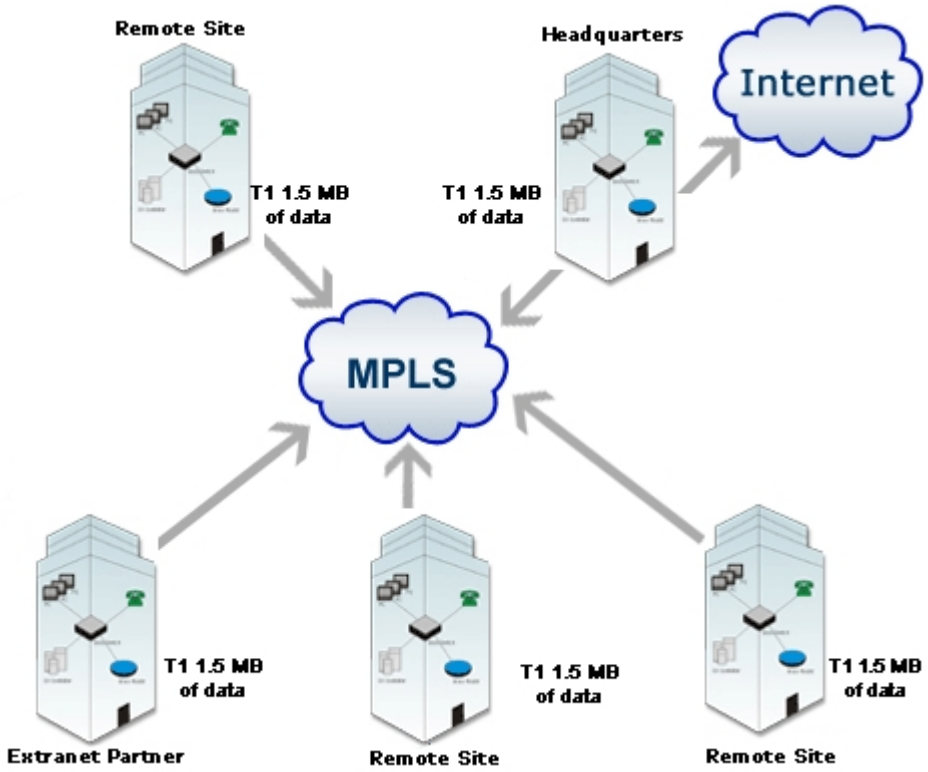
Asynchronous Transfer Mode

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 1086

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:

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

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.

Question 1087

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.

Question 1088

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 1089

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.

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

Question 1090

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 1091

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 1092

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 1093

Which of the following system and data conversion strategies provides the GREATEST redundancy?

- ☐ Direct cutover
- ☐ Pilot study
- ☐ Phased approach
- ☒ Parallel run

Explanation:

Explanation:

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

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 1094

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

Question 1095

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.

Question 1096

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 1097

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.

Question 1098

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 1099

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 1100

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 1101

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 1102

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.

Question 1103

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.

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

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