vce trainer

Reference Solution for isaca.test-king.cisa.v2020-09-04.by.maisie.1864q.vce

CISA

CISA

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

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

Exam A (1864 questions)

Question 1

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.

Question 2

Which of the following would be the MOST efficient audit approach, given that a compliance-based approach was adopted in the previous year?

- ☐ Validate all applications using test data.
- ☐ Interview systems personnel to evaluate all automated controls.
- ☐ Evaluate the controls surrounding changes to programs.
- ☒ Perform a review of significant transactions posted within the system.

Question 3

While reviewing a hot site, the IS auditor discovers that one type of hardware platform is not installed. The IS auditor should FIRST:

- ☐ recommend the purchase and installation of hardware at the hot site.
- ☐ report the finding immediately to senior IS management.
- ☒ determine the business impact of the absence of the hardware.
- ☐ establish the lead time for delivery of a new machine.

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

Question 4

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 5

When an organization outsources a payroll system to a cloud service provider, the IS auditor's PRIMARY concern should be the:

- ☐ service level agreement (SLA) is not reviewed annually.
- ☒ lack of independent assurance from a third party.
- ☐ service provider's data center is on the ground floor.
- ☐ service provider's platform is not compatible with legacy systems.

Question 6

The IS security group is planning to implement single sign-on. What is the IS auditor's PRIMARY concern?

- ☐ Integrated access rules will increase users' access privileges.
- ☐ Managing user IDs/passwords will require increased efforts.
- ☐ Integrated access rules will restrict users' access privileges.
- ☒ Compromise of a user ID/password will yield more privileges.

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

Question 7

An organization has implemented an automated match between purchase orders, goods receipts, and invoices. Which of the following risks will this control BESTmitigate?

- ☐ Customer discounts not being applied
- ☐ A legitimate transaction being paid multiple times
- ☒ Invalid payments being processed by the system
- ☐ Delay of purchase orders

Question 8

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 9

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:

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.

Reference:

CISA review manual 2014 Page number 362

Question 10

An auditor notes the administrator user ID is shared among three financial managers to perform month-end updates. Which of the following is the BEST recommendation to ensure the administrator ID in the financial system is controlled effectively?

- ☒ Implement use of individual software tokens
- ☐ Conduct employee awareness training
- ☐ Institute user ID logging and monitoring
- ☐ Ensure data in the financial systems has been classified

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

Question 11

Which of the following level in CMMI model focuses on process definition and process deployment?

- ☐ Level 4
- ☐ Level 5
- ☒ Level 3
- ☐ Level 2

Explanation:

Explanation:

Level 3 is the defined step and focus on process definition and process deployment.

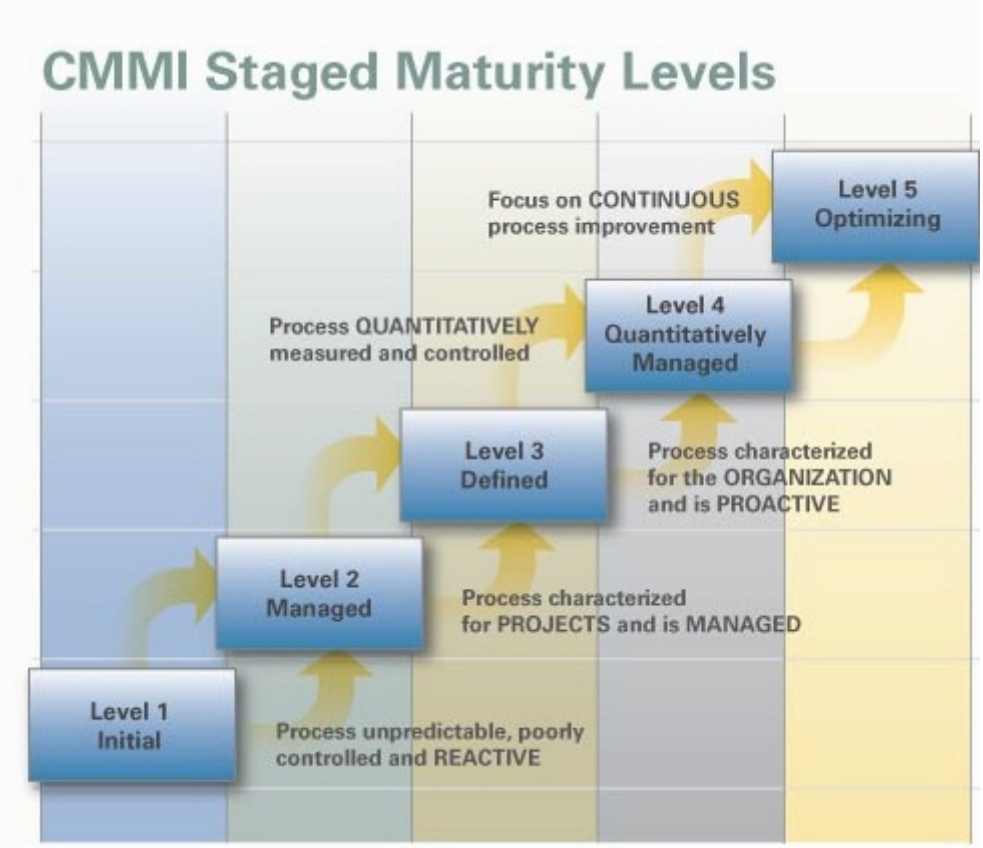
For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.

CMMI Levels

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



A maturity model can be used as a benchmark for comparison and as an aid to understanding - for example, for comparative assessment of different organizations where there is something in common that can be used as a basis for comparison. In the case of the CMM, for example, the basis for comparison would be the organizations' software development processes.

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

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

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".[citation needed]

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.

Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions).

Managed - the process is quantitatively managed in accordance with agreed-upon metrics.

Optimizing - process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

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

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

The following were incorrect answers:

Level 4 – Focus on process management and process control

Level 5 – Process innovation and continuous optimization.

Level 2 – Performance management and work product management.

Reference:

CISA review manual 2014 Page number 188

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

Question 12

An IS auditor is reviewing the upgrading of an operating system. Which of the following would be the GREATEST audit concern?

- ☐ The lack of release notes
- ☒ The lack of change control
- ☐ The lack of malware protection
- ☐ The lack of activity logging

Question 13

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 14

An IS auditor is observing transaction processing and notes that a high-priority update job ran out of sequence. What is the MOST significant risk from this observation?

- ☐ Previous jobs may have failed.
- ☐ The job may not have run to completion.
- ☐ Daily schedules may not be accurate.
- ☒ The job competes with invalid data.

Question 15

When responding to an ongoing denial of service (DoS) attack, an organization's FIRST course of action should be to:

- ☐ restore service
- ☒ minimize impact
- ☐ analyze the attack path
- ☐ investigate damage

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

Question 16

During audit planning, an IS auditor walked through the design of controls related to a new data loss prevention (DLP) tool. It was noted that the tool will be configured to alert IT management when large files are sent outside of the organization via email. What type of control will be tested?

- ☒ Detective
- ☐ Corrective
- ☐ Directive
- ☐ Preventive

Question 17

The BEST way to evaluate a shared control environment is to obtain an assurance report and review which of the following?

- ☐ Control self-assessment (CSA)
- ☐ Service level agreement (SLA)
- ☒ Master service agreement
- ☐ Complementary user entity controls

Question 18

During the review of a business process reengineering project, the PRIMARY concern of an IS auditor is to determine whether the new business model:

- ☐ is aligned with industry best practices.
- ☒ is aligned with organizational goals.
- ☐ leverages benchmarking results.
- ☐ meets its key performance measures.

Question 19

An IS auditor notes that several users have not logged into an application for more than one year. Which of the following would be the BEST audit recommendation?

- ☐ Periodically review the information security policy.
- ☐ Update the termination procedures.
- ☒ Periodically review user access.
- ☐ Delete the affected users' IDs.

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

Question 20

What is the BEST backup strategy for a large database with data supporting online sales?

- ☒ Weekly full backup with daily incremental backup
- ☐ Daily full backup
- ☐ Clustered servers
- ☐ Mirrored hard disks

Explanation:

Explanation:

Weekly full backup and daily incremental backup is the best backup strategy; it ensures the ability to recover the database and yet reduces the daily backup time requirements. A full backup normally requires a couple of hours, and therefore it can be impractical to conduct a full back up every day. Clustered servers provide a redundant processing capability, but are not a backup.

Mirrored hard disks will not help in case of disaster.

Question 21

The GREATEST risk of database denormalization is:

- ☒ decreased performance.
- ☐ loss of data confidentiality.
- ☐ loss of database integrity.
- ☐ incorrect metadata.

Question 22

During an audit of the logical access control of an ERP financial system an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. These accounts allow access to financial transactions on the ERP. What should the IS auditor do next?

- ☒ Look for compensating controls.
- ☐ Review financial transactions logs.
- ☐ Review the scope of the audit.
- ☐ Ask the administrator to disable these accounts.

Explanation:

Explanation:

The best logical access control practice is to create user IDs for each individual to define accountability. This is possible only by establishing a one-to-one relationship between IDs and individuals. However, if the user IDs are created based on role designations, an IS auditor should first understand the reasons and then evaluate the effectiveness and efficiency of compensating controls. Reviewing transactions logs is not relevant to an audit of logical access control nor is reviewing the scope of the audit relevant. Asking the administrator to disable the shared accounts should not be

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

recommended by an IS auditor before understanding the reasons and evaluating the compensating controls. It is not an IS auditor's responsibility to ask for disabling accounts during an audit.

Question 23

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 24

Which of the following activities should occur after a business impact analysis (BIA)?

- ☐ Identify threats to the IT environment
- ☐ Identify critical applications
- ☒ Analyze recovery options
- ☐ Review the computing and user environment

Question 25

Which of the following reports can MOST effectively be used to analyze a systems performance problem?

- ☐ Synchronization report
- ☒ Console log
- ☐ Utilization report
- ☐ Database usage log

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

Question 26

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 27

Which of the following is MOST efficiently protects 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 28

Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Database snapshots can provide an excellent audit trail for an IS auditor.

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

Question 29

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.

Question 30

Which of the following types of spyware was originally designed for determining the sources of error or for measuring staff productivity?

- ☐ Keywords logging
- ☒ Keystroke logging
- ☐ Directory logging
- ☐ Password logging
- ☐ None of the choices.

Explanation:

Explanation:

Keystroke logging (in the form of spyware) was originally a function of diagnostic tool deployed by software developers for capturing user's keystrokes.

This is done for determining the sources of error or for measuring staff productivity.

Question 31

Which of the following is the MOST effective control for emergency changes to application programs?

- ☒ Processing the change through change control with review of the change the following day
- ☐ Keeping a sealed envelope containing a password that operators can use to make emergency changes
- ☐ Periodically checking the application program libraries to detect whether unauthorized changes have been made
- ☐ Preparing and approving program change forms before the changes are made

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

Question 32

Of the following procedures for testing a disaster recovery plan (DRP), which should be used MOST frequently?

- ☐ Unannounced shutdown of the primary computing facility.
- ☒ Review of documented backup and recovery procedures
- ☐ Testing at a secondary site using offsite data backups
- ☐ Preplanned shutdown of the computing facility during an off-peak period

Question 33

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:

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.

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

Electronic Check Model – Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Transfer Model – Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

The following were incorrect answers:

Electronic 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.

Reference:

CISA review manual 2014 Page number 183

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

Question 34

Code changes are compiled and placed in a change folder by the developer. An implementation team migrates changes to production from the change folder. Which of the following BEST indicates separation of duties is in place during the migration process?

- ☒ A second individual performs code review before the change is released to production.
- ☐ The developer approves changes prior to moving them to the change folder.
- ☐ The implementation team does not have experience writing code.
- ☐ The implementation team does not have access to change the source code.

Question 35

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 36

An IS auditor has been asked to participate in the creation of an organization's formal business continuity program. Which of the following would impair auditor independence?

- ☒ Developing disaster recovery test scenarios
- ☐ Determining system criticality
- ☐ Facilitating the business impact analysis (BIA)
- ☐ Participating on the business continuity committee

Question 37

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

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

Question 38

Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

- ☐ Function Point Analysis (FPA)
- ☐ GANTT
- ☐ Rapid Application Development (RAD)
- ☒ PERT

Explanation:

Explanation:

PERT is a program-evaluation review technique that considers different scenarios for planning and control projects.

Question 39

Which of the following function in traditional EDI process is used for transmitting and receiving electronic documents between trading partners via dial up lines, public switched network or VAN?

- ☒ Communication handler
- ☐ EDI Interface
- ☐ Application System
- ☐ EDI Translator

Explanation:

Explanation:

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN).

For your exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's computer system

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox services similar to post offices. The VAN receives all the outbound transactions from an organization, sort them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

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

EDI Interface – Interface function that manipulates and routes data between the application system and the communication handler. The interface consists of two components

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping. Data mapping is the process by which data are extracted from EDI translation process and integrated with the data or process of receiving company.

3. Application System – The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

EDI Interface – Interface function that manipulates and routes data between the application system and the communication handler.

Application System – The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Reference:

CISA review manual 2014 Page number 178

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

Question 40

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 41

Which of the following is the BEST method for converting a file into a format suitable for data analysis in a forensic investigation?

- ☐ Extraction
- ☒ Normalization
- ☐ Data acquisition
- ☐ Imaging

Question 42

The GREATEST advantage of using web services for the exchange of information between two systems is:

- ☐ secure communications.
- ☐ improved performance.
- ☒ efficient interfacing.
- ☐ enhanced documentation.

Explanation:

Explanation:

Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

Question 43

Which of the following is the PRIMARY advantage of single sign-on (SSO)?

- ☐ Improves system performance
- ☐ Ensures good password practices
- ☐ Improves security
- ☒ Reduces administrative workload.

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

Question 44

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 45

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- ☐ Wet-pipe sprinkler system
- ☐ Dry-pipe sprinkler system
- ☒ FM-200system
- ☐ Carbon dioxide-based fire extinguishers

Explanation:

Explanation:

FM-200 is safer to use than carbon dioxide. It is considered a clean agent for use in gaseous fire suppression applications. A water-based fire extinguisher is suitable when sensitive computer equipment could be damaged before the fire department personnel arrive at the site. Manual firefighting (fire extinguishers) may not provide fast enough protection for sensitive equipment (e.g., network servers).

Question 46

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

- ☐ Cold-site facilities
- ☐ Disaster recovery for networks
- ☐ Diverse processing
- ☒ Disaster recovery for systems

Explanation:

Explanation:

Disaster recovery for systems typically focuses on making alternative processes and resources available for transaction processing.

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

Question 47

What is the MOST effective way to ensure information security incidents will be managed effectively and in a timely manner?

- ☐ Obtain senior management commitment.
- ☒ Test incident response procedures regularly.
- ☐ Communicate incident response procedures to staff.
- ☐ Establish and measure key performance indicators (KPIs).

Question 48

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 greater the sample size
- ☐ The greater the sample size, the lower the expected error rate

Question 49

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☒ MTD

Explanation:

Explanation:

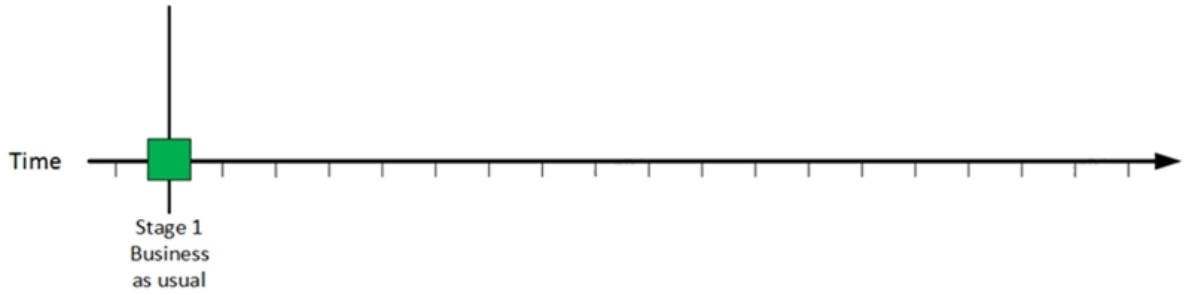
The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

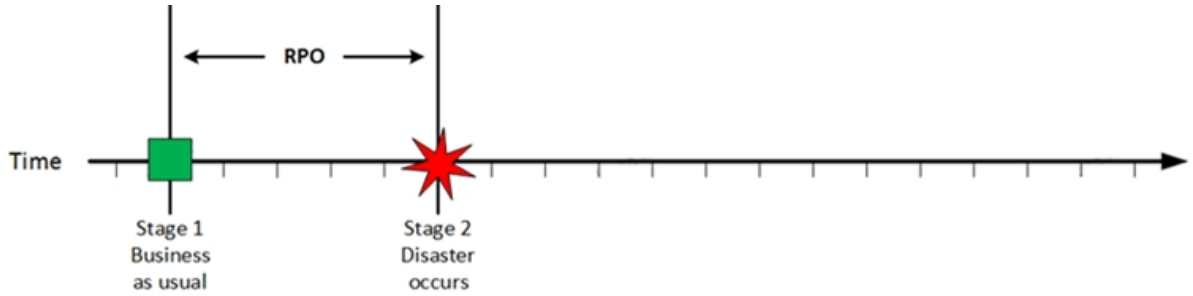
Licensed to Berend Post berend.post@it-university.nl



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

Stage 2: Disaster occurs

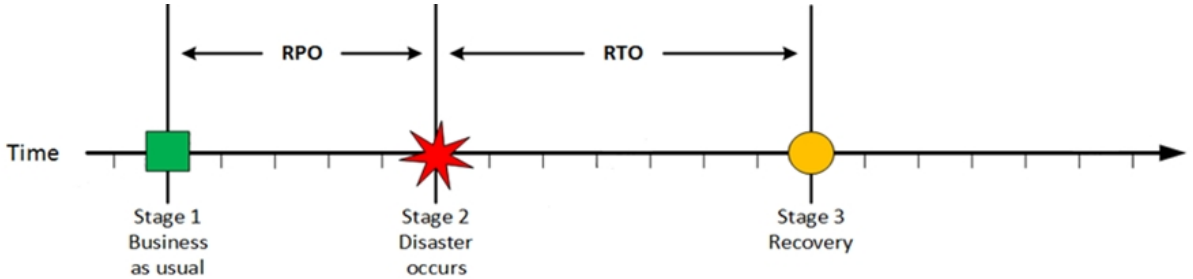
Disaster Occurs



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

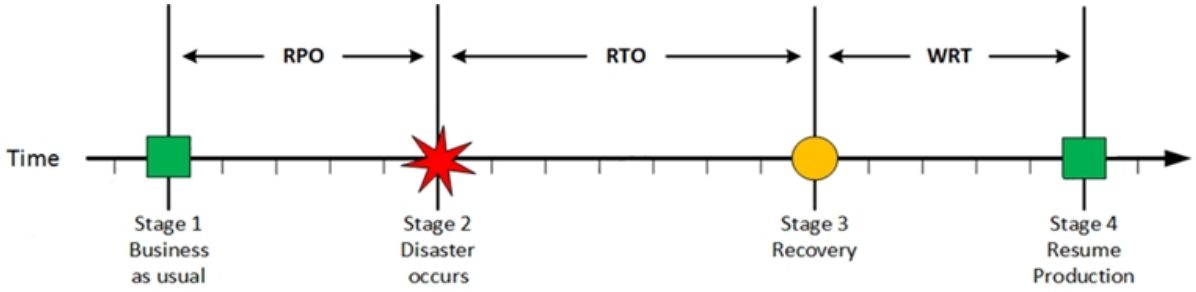


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most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

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

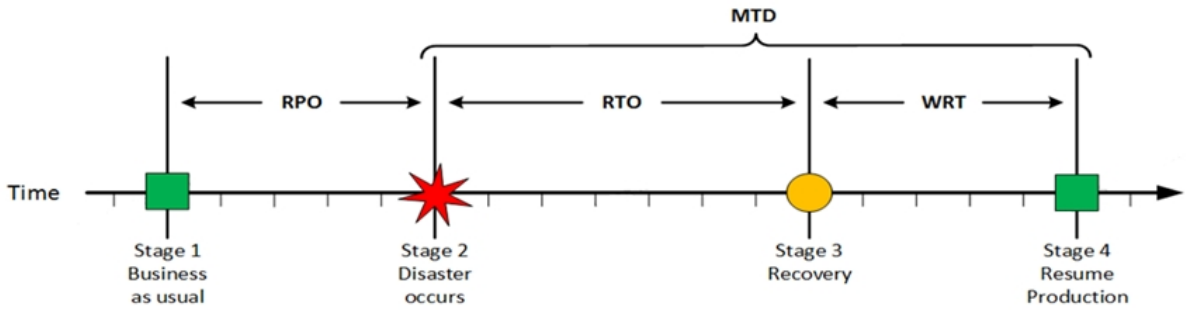
Stage 4: Resume Production

Resume Production



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

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

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

Reference:

CISA review manual 2014 page number 284

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

Question 50

Which of the following is by far the most common prevention system from a network security perspective?

- ☒ Firewall
- ☐ IDS
- ☐ IPS
- ☐ Hardened OS
- ☐ Tripwire
- ☐ None of the choices.

Explanation:

Explanation:

User account access controls and cryptography can protect systems files and data, respectively. On the other hand, firewalls are by far the most common prevention systems from a network security perspective as they can shield access to internal network services, and block certain kinds of attacks through packet filtering.

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

Question 51

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 52

A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

- ☐ Most employees use laptops.
- ☐ A packet filtering firewall is used.
- ☐ The IP address space is smaller than the number of PCs.
- ☒ Access to a network port is not restricted.

Explanation:

Explanation:

Given physical access to a port, anyone can connect to the internal network. The other choices do not present the exposure that access to a port does. DHCP provides convenience (an advantage) to the laptop users. Sharing IP addresses and the existence of a firewall can be security measures.

Question 53

When reviewing a newly implemented quality management system (QMS), which of the following should be the IS auditor's PRIMARY concern?

- ☐ The QMS benefit measures were not included in the business case.
- ☐ The QMS testing methodology is not clearly documented.
- ☐ The QMS post-implementation review (PIR) has not been finalized.
- ☒ The QMS is not mapped to some core business processes.

Question 54

The FIRST step in establishing a firewall security policy is to determine the:

- ☐ necessary logical access rights.
- ☐ expected data throughput.
- ☒ business requirements.
- ☐ existing firewall configuration.

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

Question 55

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

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

Question 56

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 57

During a review of an insurance company's claims system, the IS auditor learns that claims for specific medical procedures are acceptable only from females. This is an example of a:

- ☐ key verification.
- ☐ completeness check.
- ☒ reasonableness check.
- ☐ logical relationship check.

Question 58

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

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

Question 59

Which of the following goals would you expect to find in an organization's strategic plan?

- ☐ Test a new accounting package.
- ☐ Perform an evaluation of information technology needs.
- ☐ Implement a new project planning system within the next 12 months.
- ☒ Become the supplier of choice for the product offered.

Explanation:

Explanation:

Strategic planning sets corporate or departmental objectives into motion. Comprehensive planning helps ensure an effective and efficient organization. Strategic planning is time- and project-oriented, but also must address and help determine priorities to meet business needs. Long- and short-range plans should be consistent with the organization's broader plans for attaining their goals. Choice D represents a business objective that is intended to focus the overall direction of the business and would thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

Question 60

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 61

The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

- ☐ IT budget.
- ☐ existing IT environment.
- ☒ business plan.
- ☐ investment plan.

Explanation:

Explanation:

One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall

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

IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration. Choices A, B and D are important but secondary to the importance of reviewing the business plan,

Question 62

Which of the following would BEST provide an information security manager with sufficient assurance that a service provider complies with organization's information security requirements?

- ☐ A live demonstration of the third-party supplier's security capabilities
- ☐ Third-party security control self-assessment results
- ☒ An independent review report indicating compliance with industry standards
- ☐ The ability to audit the third-party supplier's IT systems and processes

Question 63

Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

- ☐ The disaster levels are based on scopes of damaged functions, but not on duration.
- ☐ The difference between low-level disaster and software incidents is not clear.
- ☐ The overall BCP is documented, but detailed recovery steps are not specified.
- ☒ The responsibility for declaring a disaster is not identified.

Explanation:

Explanation:

If nobody declares the disaster, the response and recovery plan would not be invoked, making all other concerns mute. Although failure to consider duration could be a problem, it is not as significant as scope, and neither is as critical as the need to have someone invoke the plan. The difference between incidents and low-level disasters is always unclear and frequently revolves around the amount of time required to correct the damage. The lack of detailed steps should be documented, but their absence does not mean a lack of recovery, if in fact someone has invoked the plan.

Question 64

An IS auditor finds that application servers had inconsistent configurations leading to potential security vulnerabilities. Which of the following should the auditor recommend FIRST?

- ☒ Enforce server baseline standards.
- ☐ Improve change management processes using a workflow tool.
- ☐ Hold the application owner accountable for monitoring metrics.
- ☐ Use a single vendor for the application servers.

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

Question 65

Which of the following is the PRIMARY role of an IS auditor with regard to data privacy?

- ☒ Ensuring compliance with data privacy laws
- ☐ Communicating data privacy requirements to the organization
- ☐ Drafting the organization's data privacy policy
- ☐ Verifying that privacy practices match privacy statements

Question 66

The independence of an IS auditor auditing an application is maintained if the auditor's role is limited to:

- ☐ creating system specifications.
- ☒ defining user requirements.
- ☐ recommending system enhancements.
- ☐ designing access control rules.

Question 67

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 68

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 69

When reviewing the process by which a contract for the outsourcing of various IT functions was completed, an IS auditor would ensure that the successful contractor:

- ☐ has eliminated the risks of outsourcing.
- ☒ maintains an internal audit function.
- ☐ requires a confidentiality agreement to be signed by all employees.
- ☐ was selected according to established business criteria.

Question 70

Which of the following audit mainly focuses on discovering and disclosing on frauds and crimes?

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

Explanation:

Explanation:

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

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

What is an audit?

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

Compliance Audit

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

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

specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

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

Financial Audit

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

Operational Audit

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

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

Objectives

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

To understand the responsibilities and risks faced by an organization.

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

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

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

Integrated Audits

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

IS Audit

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

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

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

Forensic Audit

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

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

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

The following answers are incorrect:

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

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

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

Reference:

CISA Review Manual 2014 Page number 44

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

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

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

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

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

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

Question 71

When auditing the effectiveness of a biometric system, which of the following indicators would be MOST important to review?

- ☐ False negatives
- ☒ False acceptance rate
- ☐ Failure to enroll rate
- ☐ System response time

Question 72

The PRIMARY objective of implementing corporate governance by an organization's management is to:

- ☒ provide strategic direction.
- ☐ control business operations.
- ☐ align IT with business.
- ☐ implement best practices.

Explanation:

Explanation:

Corporate governance is a set of management practices to provide strategic direction, thereby ensuring that goals are achievable, risks are properly addressed and organizational resources are properly utilized. Hence, the primary objective of corporate governance is to provide strategic direction. Based on the strategic direction, business operations are directed and controlled.

Question 73

An IS auditor is evaluating a virtual server environment and learns that the production server, development server, and management console are housed in the same physical host. What should be the auditor's PRIMARY concern?

- ☒ The physical host is a single point of failure
- ☐ The management console is a single point of failure
- ☐ The development server and management console share the same host
- ☐ The development and production servers share the same host

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

Question 74

Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

- ☐ Senior management is aware of critical information assets and demonstrates an adequate concern for their protection.
- ☒ Job descriptions contain clear statements of accountability for information security.
- ☐ In accordance with the degree of risk and business impact, there is adequate funding for security efforts.
- ☐ No actual incidents have occurred that have caused a loss or a public embarrassment.

Explanation:

Explanation:

Inclusion in job descriptions of security responsibilities is a form of security training and helps ensure that staff and management are aware of their roles with respect to information security. The other three choices are not criterion for evaluating security awareness training. Awareness is a criterion for evaluating the importance that senior management attaches to information assets and their protection. Funding is a criterion that aids in evaluating whether security vulnerabilities are being addressed, while the number of incidents that have occurred is a criterion for evaluating the adequacy of the risk management program.

Question 75

Which of the following would protect the confidentiality of information sent in email messages?

- ☒ Encryption
- ☐ Digital certificates
- ☐ Digital signatures
- ☐ Secure Hash Algorithm 1 (SHA-1)

Question 76

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:

Explanation:

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

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 77

Which of the following should be considered when examining fire suppression systems as part of a data center environmental controls review?

- ☒ Maintenance procedures
- ☐ Onsite replacement availability
- ☐ Insurance coverage
- ☐ Installation manuals

Question 78

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

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

Explanation:

Explanation:

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

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

Question 79

Codes from exploit programs are frequently reused in:

- ☐ trojan horses only.
- ☐ computer viruses only.
- ☐ OS patchers.
- ☐ eavedroppers.
- ☒ trojan horses and computer viruses.
- ☐ None of the choices.

Explanation:

Explanation:

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

Question 80

An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

- ☐ Recommend that an additional comprehensive BCP be developed.
- ☒ Determine whether the BCPs are consistent.
- ☐ Accept the BCPs as written.
- ☐ Recommend the creation of a single BCP.

Explanation:

Explanation:

Depending on the complexity of the organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan; however, each plan should be consistent with other plans to have a viable business continuity planning strategy.

Question 81

Data edits are implemented before processing and are considered which of the following?

- ☐ Deterrent integrity controls
- ☐ Detective integrity controls
- ☐ Corrective integrity controls
- ☒ Preventative integrity controls

Explanation:

Explanation:

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

Data edits are implemented before processing and are considered preventive integrity controls.

Question 82

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 83

A configuration management audit identified that predefined automated procedures are used when deploying and configuring application infrastructure in a cloud-based environment. Which of the following is MOST important for the IS auditor to review?

- ☐ Contracts of vendors responsible for maintaining provisioning tools
- ☒ Processes for making changes to cloud environment specifications
- ☐ Storage location of configuration management documentation
- ☐ Number of administrators with access to cloud management consoles

Question 84

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.

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

Question 85

Which of the following tools is MOST helpful in estimating budgets for tasks within a large IT business application project?

- ☐ Balanced scorecard
- ☒ Gantt chart
- ☐ Function point analysis (FPA)
- ☐ Critical path methodology (CPM)

Question 86

Identify the correct sequence of Business Process Reengineering (BPR) benchmarking process from the given choices below?

- ☒ PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE
- ☐ OBSERVE, PLAN, RESEACH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, OBSERVE, RESEARCH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, RESEARCH, ANALYZE, OBSERVE, ADOPT and IMPROVE

Explanation:

Explanation:

The correct sequence of BRP benchmarking is PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE.

For your exam you should know the information below:

Overview of Business Process Reengineering

One of the principles in business that remains constant is the need to improve your processes and procedures. Most trade magazines today contain discussions of the detailed planning necessary for implementing change in an organization. The concept of change must be accepted as a fundamental principle. Terms such as business evolution and continuous improvement ricochet around the room in business meetings. It's a fact that organizations which fail to change are destined to perish.

As a CISA, you must be prepared to investigate whether process changes within the organization are accounted for with proper documentation. All internal control frameworks require that management be held responsible for safeguarding all the assets belonging to their organization. Management is also responsible for increasing revenue.

BPR Application Steps

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

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.

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

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

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

Execution of conversion plan with progress monitoring

Training of users and support personnel

Pilot implementation to ensure a smooth migration Formal approval by the sponsor.

The reconstructed process must be formally approved by management to witness their consent for fitness of use. IT governance dictates that executive management shall be held responsible for any failures and receive recognition for exceptional results. System performance will be evaluated again after entering production use.

Evaluate (post evaluation) The reconstructed process is monitored to ensure that it works and is producing the strategic value as forecast in the original justification.

Comparison of original forecast to actual performance Identification of lessons learned

Total quality management plan to maintain the new process

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

A method of continuous improvement is implemented to track the original goals against actual process performance. Annual reevaluation is needed to adapt new requirements or new opportunities.

Benchmarking as a BPR Tool

Benchmarking is the process of comparing performance data (aka metrics). It can be used to evaluate business processes that are under consideration for reengineering. Performance data may be obtained by using a self-assessment or by auditing for compliance against a standard (reference standard). Evidence captured during the diagnostic phase is considered the key to identifying areas for performance improvement and documenting obstacles. ISACA offers the following general guidelines for performing benchmarks:

Plan Identify the critical processes and create measurement techniques to grade the processes.

Research Use information about the process and collect regular data (samples) to build a baseline for comparison. Consider input from your customers and use analogous data from other industries.

Observe Gather internal data and external data from a benchmark partner to aid the comparison results. Benchmark data can also be compared against published standards.

Analyze Look for root cause-effect relationships and other dependencies in the process. Use predefined tools and procedures to collate the data collected from all available sources.

Adapt Translate the findings into hypotheses of how these findings will help or hurt strategic business goals. Design a pilot test to prove or disprove the hypotheses.

Improve Implement a prototype of the new processes. Study the impact and note any unexpected results. Revise the process by using controlled change management. Measure the process results again. Use reestablished procedures such as total quality management for continuous improvement.

The following answers are incorrect:

The other options specified does not represent the correct sequence of BRP benchmarking steps.

Reference:

CISA review manual 2014 page number 219 to 211

CISA certified information system auditor study guide Second Edition Page Number 154 to 158

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

Question 87

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 88

Which of the following should be of GREATEST concern to an IS auditor reviewing actions taken during a forensic investigation?

- ☐ The investigation report does not indicate a conclusion.
- ☐ An image copy of the attacked system was not taken.
- ☒ The proper authorities were not notified.
- ☐ The handling procedures of the attacked system are not documented.

Question 89

A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:

- ☒ analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
- ☐ WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.
- ☐ the line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
- ☐ users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

Explanation:

Explanation:

The peak at 96 percent could be the result of a one-off incident, e.g., a user downloading a large amount of data; therefore, analysis to establish whether this is a regular pattern and what causes this behavior should be carried out before expenditure on a larger line capacity is recommended.

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

Since the link provides for a standby database, a short loss of this service should be acceptable. If the peak is established to be a regular occurrence without any other opportunities for mitigation (usage of bandwidth reservation protocol, or other types of prioritizing network traffic), the line should be replaced as there is the risk of loss of service as the traffic approaches 100 percent. If, however, the peak is a one-off or can be put in other time frames, then user education may be an option.

Question 90

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 91

An IS auditor considering use of another auditor's workpapers should:

- ☐ rarely rely on the work of another auditor.
- ☐ determine that the workpapers were completed within the past month.
- ☒ determine that then auditee agrees with key issues in these workpapers.
- ☐ consider the appropriateness and sufficiency of the workpapers.

Question 92

A data administrator is responsible for:

- ☐ maintaining database system software.
- ☒ defining data elements, data names and their relationship.
- ☐ developing physical database structures.
- ☐ developing data dictionary system software.

Explanation:

Explanation:

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

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

Question 93

During an incident management audit, an IS auditor finds that several similar incidents were logged during the audit period. Which of the following is the auditor's MOST important course of action?

- ☐ Document the finding and present it to management.
- ☐ Determine if a root cause analysis was conducted.
- ☒ Validate whether all incidents have been actioned.
- ☐ Confirm the resolution time of the incidents.

Question 94

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:

Explanation:

A modem is a device that translates data from digital form and then back to digital for communication over analog lines.

Reference: Information Systems Audit and Control Association,

Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

Question 95

Which of the following is the PRIMARY function of technology-driven enterprise architecture?

- ☐ To provide guidance on technological decisions in the context of business strategy
- ☐ To determine how new technologies fit into existing networks and data flows
- ☐ To help develop project documentation and related business process roadmaps
- ☒ To re-engineer business processes to make better use of technology

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

Question 96

An organization allows employee use of personal mobile devices for corporate email. Which of the following should be the GREATEST IS audit concern?

- ☐ Email forwarding to private devices requires excessive network bandwidth
- ☒ There is no corporate policy for the acceptable use of private devices
- ☐ There is no adequate tracking of the working time spent out-of-hours
- ☐ The help desk is not able to fully support different kinds of private devices

Question 97

A firewall has been installed on the company's web server. Which concern does the firewall address?

- ☐ Availability of the information
- ☐ Unauthorized modification of information by internal users
- ☒ Accessing information by the outside world
- ☐ Connectivity to the Internet

Question 98

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:

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.

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

Management of IT and Enterprise Architecture: A verification that the in-place IT management infrastructure encompassing all aspects of system support has been put in place. This is to ensure effective change control, audit, business continuity and security procedures etc. have been formulated, documented and put in place.

Interconnection Policy: A verification that adequate security and business continuity controls governing the connection to other systems, be they Telecommunications, Intranets, Extranets and Internet etc. have been put in place, have been fully documented and correspond to the stated customer requirements.

The following answers are incorrect:

Substantive testing - A procedure used during accounting audits to check for errors in balance sheets and other financial documentation. A substantive test might involve checking a random sample of transactions for errors, comparing account balances to find discrepancies, or analysis and review of procedures used to execute and record transactions.

Sanity testing - Testing to determine if a new software version is performing well enough to accept it for a major testing effort. If application is crashing for initial use, then system is not stable enough for further testing and build or application is assigned to fix.

Recovery testing – Testing how well a system recovers from crashes, hardware failures, or other catastrophic problems.

Reference:

CISA review manual 2014 page number 52 and 53

http://www.wikijob.co.uk/wiki/substantive-testing

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

Question 99

What is the BEST way for an IS auditor to address the risk associated with over-retention of personal data after identifying a large number of customer records retained beyond the retention period defined by law?

- ☒ Recommend automating deletion of records beyond the retention period.
- ☐ Schedule regular internal audits to identify records for deletion.
- ☐ Report the retention period noncompliance to the regulatory authority.
- ☐ Escalate the over-retention issue to the data privacy officer for follow-up.

Question 100

Which of the following would present the GREATEST need to revise information security policies?

- ☐ An increase in reported incidents
- ☒ A merger with a competing company
- ☐ Implementation of a new firewall
- ☐ Changes in standards and procedures

Question 101

Which of the following BEST facilitates the ability to efficiently allocate time, effort, and resources to address security incidents?

- ☒ Incident classification
- ☐ Incident definition
- ☐ Incident escalation
- ☐ Incident monitoring

Question 102

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:

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.

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

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition."

The steps in each successive PDCA cycle are:

PLAN

Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals). By establishing output expectations, the completeness and accuracy of the spec is also a part of the targeted improvement. When possible start on a small scale to test possible effects.

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

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

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

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

Reference:

CISA review manual 2014 page number 107

Question 103

What is the PRIMARY reason for hardening new devices before introducing into a corporate network?

- ☐ To comply with organizational rules
- ☐ To ease maintenance of devices
- ☒ To reduce exposure to attacks
- ☐ To avoid software licensing conflicts

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

Question 104

Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

- ☐ poorer performance.
- ☐ poor scalability.
- ☐ weak infrastructure.
- ☒ high costs in terms of training and maintenance.
- ☐ None of the choices.

Explanation:

Explanation:

An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.

Question 105

Which of the following type of IDS has self-learning functionality and over a period of time will learned what is the expected behavior of a system?

- ☐ Signature Based IDS
- ☐ Host Based IDS
- ☒ Neural Network based IDS
- ☐ Statistical based IDS

Explanation:

Explanation:

Neural Network based IDS monitors the general patterns of activity and traffic on the network, and create a database of normal activities within the system. This is similar to statistical model but with added self-learning functionality.

Also, you should know below categories and types of IDS for CISA exam:

An IDS works in conjunction with routers and firewall by monitoring network usage anomalies.

Broad category of IDS includes:

Network based IDS

Host based IDS

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

Network Based IDS

They identify attack within the monitored network and issue a warning to the operator.

If a network based IDS is placed between the Internet and the firewall, it will detect all the attack attempts whether or not they enter the firewall

Host Based IDS

They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack.

They can detect the modification of executable programs, detect the detection of files and issue a warning when an attempt is made to use a privilege account.

Types of IDS includes

Signature Based IDS – These IDS system protect against detected intrusion patterns. The intrusive pattern they can identify are stored in the form of signature.

Statistical Based IDS – This system needs a comprehensive definition of the known and expected behavior of system

Neural Network – An IDS with this feature monitors the general patterns of activity and traffic on the network, and create a database. This is similar to statistical model but with added self-learning functionality

The following were incorrect answers:

The other types of IDS mentioned in the options do not monitor general patterns of activities and contains self-learning functionalities.

Reference:

CISA review manual 2014 Page number 346 and 347

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

Question 106

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 107

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

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

Explanation:

Explanation:

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

Question 108

An IS auditor is evaluating the log management system for an organization with devices and systems in multiple geographic locations. Which of the following is MOST important for the auditor to verify?

- ☐ Log files are encrypted and digitally signed.
- ☒ Log files of the servers are synchronized.
- ☐ Log files are reviewed in multiple locations.
- ☐ Log files are concurrently updated.

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

Question 109

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

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

Question 110

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 111

To provide protection for media backup stored at an offsite location, the storage site should be:

- ☐ located on a different floor of the building.
- ☐ easily accessible by everyone.
- ☐ clearly labeled for emergency access.
- ☒ protected from unauthorized access.

Explanation:

Explanation:

The offsite storage site should always be protected against unauthorized access and have at least the same security requirements as the primary site. Choice A is incorrect because, if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.

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

Question 112

As part of a mergers and acquisitions activity, an acquiring organization wants to consolidate data and system from the organization being acquired into existing systems. To ensure the data is relevant, the acquiring organization should:

- ☐ obtain data quality software.
- ☒ define data quality requirements based on business needs.
- ☐ automate the process of data collection and cleaning.
- ☐ implement a data warehouse solution.

Question 113

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 114

A PRIMARY benefit derived by an organization employing control self-assessment (CSA) techniques is that CSA:

- ☒ can identify high-risk areas for detailed review.
- ☐ allows IS auditors to independently assess risk.
- ☐ can be used as a replacement for traditional audits.
- ☐ allows management to relinquish responsibility for control.

Explanation:

Explanation:

CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Choice B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Choice C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for control.

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

Question 115

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:

Explanation:

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

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

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

Knowledge is acquired and used

Goals are generated and achieved

Information is communicated

Collaboration is achieved

Concepts are formed

Languages are developed

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

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

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

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:

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.

Reference:

CISA review manual 2014 Page number 187

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

Question 116

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:

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.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

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

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

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

Reference:

CISA review manual 2014 page number 275

Question 117

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

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

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 118

The PRIMARY benefit of using secure shell (SSH) to access a server on a network is that it:

- ☐ provides better session reliability.
- ☐ prevents man-in-the-middle attacks.
- ☒ provides confidentiality of transmitted data.
- ☐ facilitates communication across platforms.

Question 119

Which of the following is the BEST indication that a newly developed information system is ready for migration into production?

- ☐ Items in the work breakdown structure are completed.
- ☐ Audit has signed off.
- ☒ User acceptance testing is successfully completed.
- ☐ Technical requirements are met.

Question 120

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 121

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

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

Explanation:

Explanation:

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

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

Question 122

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 123

The MOST important success factor in planning a penetration test is:

- ☐ the documentation of the planned testing procedure.
- ☐ scheduling and deciding on the timed length of the test.
- ☒ the involvement of the management of the client organization.
- ☐ the qualifications and experience of staff involved in the test.

Explanation:

Explanation:

The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

Question 124

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:

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

Explanation:

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

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.

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

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

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

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer – his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

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

Reference:

CISA review manual 2014 Page number 188

Question 125

Physical access controls are usually implemented based on which of the following means (Choose two.):

- ☒ mechanical locks
- ☒ guards
- ☐ operating systems
- ☐ transaction applications
- ☐ None of the choices.

Explanation:

Explanation:

In physical security, access control refers to the practice of restricting entrance to authorized persons. Human means of enforcement include guard, bouncer, receptionist ... etc. Mechanical means may include locks and keys.

Question 126

Which are the two primary types of scanner used for protecting against Malware?

- ☒ Malware mask/signatures and Heuristic Scanner
- ☐ Active and passive Scanner
- ☐ Behavioral Blockers and immunizer Scanner
- ☐ None of the above

Explanation:

Explanation:

Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a

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

high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

For CISA exam you should know below mentioned different kinds of malware Controls

A. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other types of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker – Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker – Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

The following were incorrect answers:

The other options presented are not a valid primary types of scanner.

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

Reference:

CISA review manual 2014 Page number 354 and 355

Question 127

Which of the following is MOST important for an IS auditor to consider when auditing a vulnerability scanning software solution?

- ☐ The scanning software was purchased from an approved vendor.
- ☐ The scanning software was approved for release into production.
- ☒ The scanning software covers critical systems.
- ☐ The scanning software is cost-effective.

Question 128

Which of the following should an IS auditor expect to find when reviewing IT security policy?

- ☒ Assigned responsibility for safeguarding company assets
- ☐ A risk-based classification of systems
- ☐ An inventory of information assets
- ☐ Virus protection implementation strategies

Question 129

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

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

Explanation:

Explanation:

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

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

Question 130

When providing a vendor with data containing personally identifiable information (PII) for offsite testing, the data should be:

- ☐ current
- ☒ encrypted.
- ☐ sanitized.
- ☐ backed up.

Question 131

Which of the following is the MOST reliable way for an IS auditor to evaluate the operational effectiveness of an organization's data loss prevention (DLP) controls?

- ☐ Verify that confidential files cannot be transmitted to a personal USB device.
- ☐ Conduct interviews to identify possible data protection vulnerabilities.
- ☒ Review data classification levels based on industry best practice.
- ☐ Verify that current DLP software is installed on all computer systems.

Question 132

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.

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

Question 133

Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?

1. Theft of service
2. Disclosure of information
3. Data Modifications
4. Denial of service
5. Traffic Analysis

- ☐ 3 and 4
- ☐ 4 and 5
- ☐ 1-4
- ☒ They are ALL risks associated with PBX

Explanation:

Explanation:

The NOT is a keyword used in the question. You need to find out the risks which are NOT associated with PBX. All the risk listed within the options are associated with PBX.

The threat of the PBX telephone system is many, depending on the goals of these attackers, and include:

Theft of service – Toll fraud, probably the most common of motives for attacker.

Disclosure of Information – Data disclosed without authorization, either by deliberate actionably accident. Examples includes eavesdropping on conversation and unauthorized access to routing and address data.

Data Modification – Data altered in some meaningful way by recording, deleting or modifying it. For example, an intruder may change billing information or modify system table to gain additional services.

Unauthorized access – Actions that permit an unauthorized user to gain access to system resources or privileges.

Denial of service – Actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.

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

Traffic Analysis – A form of passive attack in which an intruder observes information about calls and make inferences, e.g. from the source and destination number or frequency and length of messages. For example, an intruder observes a high volume of calls between a company's legal department and patent office, and conclude that a patent is being filed.

The following were incorrect answers:

All the risks presented in options are associated with PBX. So other options are not valid.

Reference:

CISA review manual 2014 Page number356

Question 134

Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

- ☐ Call forwarding
- ☒ Privacy release
- ☐ Tenanting
- ☐ Voice mail

Explanation:

Explanation:

Privacy release supports shared extensions among several devices, ensuring that only one device at a time can use an extension.

For your exam you should know below mentioned PBX features and Risks:

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

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

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

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

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

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

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

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

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:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting -Limits system user access to only those users who belong to the same tenant group – useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Reference:

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

CISA review manual 2014 Page number358

Question 135

Which of the following should an IS auditor review FIRST when evaluating incident management procedures?

- ☐ Command center monitoring
- ☐ Root cause analysis steps
- ☒ Prioritization criteria
- ☐ Peer review requirements

Question 136

Which of the following is an IS auditor's BEST recommendation for mitigating risk associated with rapid expansion of hosts within a virtual environment?

- ☐ Limit access to the hypervisor operating system (OS) and administration console
- ☐ Ensure quick access to updated images of a guest operating system for fast recovery
- ☐ Consider using a third-party service provider to share the virtual machine (VM) risk
- ☒ Implement policies and processes to control virtual machine (VM) lifecycle management

Question 137

An internal review reveals an out-of-support human resources system. Which of the following is MOST important to determine when evaluating the associated risk?

- ☐ Frequency of outages associated with the out-of-support system
- ☐ The number of people accessing the out-of-support system
- ☐ Exposure of the out-of-support system outside of the network
- ☒ Timeline to replace the out-of-support system

Question 138

An accurate biometric system usually exhibits (Choose two.):

- ☒ low EER
- ☒ low CER
- ☐ high EER
- ☐ high CER
- ☐ None of the choices.

Explanation:

Explanation:

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

One most commonly used measure of real-world biometric systems is the rate at which both accept and reject errors are equal: the equal error rate (EER), also known as the cross-over error rate (CER). The lower the EER or CER, the more accurate the system is considered to be.

Question 139

An organization is considering replacing physical backup tapes stored offsite with real-time on-line backup to a storage area network (SAN) located in the primary data center. Which of the following is the GREATEST risk?

- ☐ Archived data may not satisfy data retention requirements
- ☒ A single disaster could cause significant data loss
- ☐ Backups may require excessive storage space
- ☐ Implementation could cause significant cost increases

Question 140

Which of the following is the MOST effective way for an IS auditor to identify unauthorized changes to the production state of a critical business application?

- ☐ Run an automated scan of the production environment to detect missing software patches.
- ☐ Compare a list of production system changes with the configuration management database (CMDB).
- ☐ Review recently approved changes to application programming interfaces (API) in the production environment.
- ☒ Review recent updates in the configuration management database (CMDB) for compliance with IT policies.

Question 141

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.

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

Question 142

The PRIMARY reason for allocating sufficient time between the "go-live" phase of a new system and conducting a post-implementation review is to:

- ☐ update project requirements and design documentation
- ☐ increase availability of system implementation team resources
- ☒ allow the system to stabilize in production
- ☐ obtain sign-off on the scope of post-implementation review

Question 143

Which of the following is an IS auditor's BEST course of action upon learning that preventive controls have been replaced with detective and corrective controls?

- ☐ Report the issue to management as the risk level has increased.
- ☐ Recommend the implementation of preventive controls in addition to the other controls.
- ☐ Verify the revised controls enhance the efficiency of related business processes.
- ☒ Evaluate whether new controls manage the risk at an acceptable level.

Question 144

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

- ☒ Availability of online network documentation
- ☐ Support of terminal access to remote hosts
- ☐ Handling file transfer between hosts and interuser communications
- ☐ Performance management, audit and control

Explanation:

Explanation:

Network operating system user features include online availability of network documentation. Other features would be user access to various resources of network hosts, user authorization to access particular resources, and the network and host computers used without special user actions or commands. Choices B, C and D are examples of network operating systems functions.

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

Question 145

"Under the concept of ""defense in depth"", subsystems should be designed to:"

- ☐ ""fail insecure"""
- ☒ ""fail secure"""
- ☐ ""react to attack"""
- ☐ ""react to failure"""
- ☐ None of the choices.

Explanation:

Explanation:

"With 0""defense in depth"", more than one subsystem needs to be compromised to compromise the security of the system and the information it holds. Subsystems should default to secure settings, and wherever possible should be designed to ""fail secure"" rather than ""fail insecure"".

Question 146

Which of the following is a tool you can use to simulate a big network structure on a single computer?

- ☐ honeymoon
- ☐ honeytrap
- ☐ honeytube
- ☒ honeyd
- ☐ None of the choices.

Explanation:

Explanation:

honeyd is a GPL licensed software you can use to simulate a big network structure on a single computer.

Question 147

Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?

- ☐ Defining the business recovery plan with the IT service provider
- ☐ Requiring an external security audits of the IT service provider
- ☐ Defining information security requirements with internal IT
- ☒ Requiring regular reporting from the IT service provider

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

Question 148

A recent audit concluded that an organization's information security system was weak and that monitoring would likely fail to detect penetration. Which of the following would be the MOST appropriate recommendation?

- ☐ Look continually for new criminal behavior and attacks on sensitive data
- ☐ Establish a clear policy related to security and the handling of sensitive data
- ☒ Encrypt sensitive data while strengthening the system
- ☐ Identify and periodically remove sensitive data that is no longer needed

Question 149

An organization has software that is not compliant with data protection requirements. To help ensure that appropriate and relevant data protection controls are implemented in the future, the auditor's BEST course of action would be to:

- ☒ conduct a privacy impact assessment to identity gaps in the organization's privacy.
- ☐ recommend that privacy checks are included within the solution development life cycle.
- ☐ recommend an executive be appointed to oversee privacy program improvements.
- ☐ map the organization's business processes to identify personally identifiable information (PII).

Question 150

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

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

Question 151

An IS auditor reviewing the risk assessment process of an organization should FIRST:

- ☐ identify the reasonable threats to the information assets.
- ☐ analyze the technical and organizational vulnerabilities.
- ☒ identify and rank the information assets.
- ☐ evaluate the effect of a potential security breach.

Explanation:

Explanation:

Identification and ranking of information assets-e.g., data criticality, locations of assets-will set the tone or scope of how to assess risk in relation to the organizational value of the asset. Second, the threats facing each of the organization's assets should be analyzed according to their value to the

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

organization. Third, weaknesses should be identified so that controls can be evaluated to determine if they mitigate the weaknesses. Fourth, analyze how these weaknesses, in absence of given controls, would impact the organization information assets.

Question 152

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 153

Who is responsible for providing adequate physical and logical security for IS program, data and equipment?

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

Explanation:

Explanation:

Security administrator are responsible for providing adequate physical and logical security for IS programs, data and equipment.

For CISA exam you should know below roles in an organization

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.

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

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.

Reference:

CISA review manual 2014 Page number 361

Question 154

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."

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

Question 155

A virus typically consists of what major parts (Choose three.):

- ☒ a mechanism that allows them to infect other files and reproduce" a trigger that activates delivery of a "payload""
- ☒ a payload
- ☒ a signature
- ☐ None of the choices.

Explanation:

Explanation:

"A virus typically consist of three parts, which are a mechanism that allows them to infect other files and reproduce a trigger that activates delivery of a "payload" and the payload from which the virus often gets its name. The payload is what the virus does to the victim file."

Question 156

Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

- ☐ Analyzer
- ☐ Administration console
- ☐ User interface
- ☒ Sensor

Explanation:

Explanation:

Sensors are responsible for collecting data. Analyzers receive input from sensors and determine intrusive activity. An administration console and a user interface are components of an IDS.

Question 157

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.

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

Question 158

Which of the following is the MOST important benefit of involving IS audit when implementing governance of enterprise IT?

- ☐ Identifying relevant roles for an enterprise IT governance framework
- ☐ Verifying that legal, regulatory and contractual requirements are being met
- ☐ Making decisions regarding risk response and monitoring of residual risk
- ☒ Providing independent and objective feedback to facilitate improvement of IT processes

Question 159

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 160

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 161

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

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

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 162

The risk that is created if a single sign-on is implemented for all systems is that a/an:

- ☐ user can bypass current access security.
- ☒ compromised password gives access to all systems.
- ☐ authorized user can bypass the security layers.
- ☐ user has equivalent access on all systems.

Question 163

Which of the following should be a PRIMARY control objective when designing controls for system interfaces?

- ☐ Ensure peer-to-peer data transfers are minimized.
- ☒ Ensure all data transferred through system interfaces is encrypted.
- ☐ Ensure managed file transfer (MFT) systems have restart capability for interruptions.
- ☐ Ensure data on the sending system is identical to the data on the receiving system.

Question 164

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

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

Question 165

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:

Explanation:

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

Electronic systems are simplest of three payment models. The payer simply creates a payment transfer instructions, sign it digitally and send it to issuer. The issuer then verifies the signature on the request and performs the transfer. This type of systems requires payer to be on-line and not payee.

For CISA exam you should know below information about payment systems

There are two types of parties involved in all payment systems – the issuer and the user. An issuer is an entity that operates the payment service. An issuer holds the items that the payment represents. The user of the payment service performs two main functions – making payments and receiving payments – and therefore can be described as a payer or payee receptively.

Electronic Money Model – The objective of electronic money systems is emulating physical cash. An issuer attempts to do this by creating digital certificates, which are then purchased by users who redeem them with the issuer at a later date. In the interim, certificates can be transferred among users to trade for goods or services. For the certificate to take on some of the attributes of physical cash, certain techniques are used so that when a certificate is deposited, the issuer can not determine the original withdrawer of the certificate. This provides an electronic certificate with unconditional uncertainty.

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.

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

Electronic Check Model – Electronic check system model real-world checks quite well and thus relatively simple to understand and implement. A users write an electronic check, which is digitally signed instruction to pay. This is transferred to another user, who then deposits the electronic check with the issuer. The issuer will verify payer's signature on the payment and transfer the fund from the payer's account to the payee's account.

Electronic Withdraw Model – Not a valid type of payment system.

Reference:

CISA review manual 2014 Page number 183

Question 166

Parity bits are a control used to validate:

- ☐ Data authentication
- ☒ Data completeness
- ☐ Data source
- ☐ Data accuracy

Explanation:

Explanation:

Parity bits are a control used to validate data completeness.

Question 167

The human resources (HR) department has developed a system to allow employees to enroll in benefits via a web site on the corporate Intranet. Which of the following would protect the confidentiality of the data?

- ☒ SSL encryption
- ☐ Two-factor authentication
- ☐ Encrypted session cookies
- ☐ IP address verification

Explanation:

Explanation:

The main risk in this scenario is confidentiality, therefore the only option which would provide confidentiality is Secure Socket Layer (SSL) encryption. The remaining options deal with authentication issues.

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

Question 168

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:

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:

Policy and standard

Proper authorization

Identification and authentication mechanism

Encryption tool and technique such as use of VPN

System and network management

Reference:

CISA Review Manual 2014 Page number 334

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

Question 169

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 170

Which of the following roles is BEST suited to assign classification to an information asset?

- ☒ The data owner
- ☐ The information security manager
- ☐ The data custodian
- ☐ The senior manager

Question 171

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- ☐ A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- ☐ Firewall policies are updated on the basis of changing requirements.
- ☐ inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- ☒ The firewall is placed on top of the commercial operating system with all installation options.

Explanation:

Explanation:

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options

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

available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

Question 172

Which of the following terms is used more generally for describing concealment routines in a malicious program?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☒ rootkits
- ☐ backdoor
- ☐ None of the choices.

Explanation:

Explanation:

Rootkits can prevent a malicious process from being reported in the process table, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator access. Today, the term is used more generally for concealment routines in a malicious program.

Question 173

A security review focused on data loss prevention (DLP) revealed the organization has no visibility to data stored in the cloud. What is the IS auditor's BEST recommendation to address this issue?

- ☐ Implement a file system scanner to discover data stored in the cloud.
- ☐ Utilize a DLP tool on desktops to monitor user activities.
- ☒ Employ a cloud access security broker (CASB).
- ☐ Enhance the firewall at the network perimeter.

Question 174

A review of Internet security disclosed that users have individual user accounts with the Internet service providers (ISPs) and use these accounts for downloading business data. The organization wants to ensure that only corporate network is used. The organization should FIRST:

- ☐ use a proxy server to filter out Internet sites that should not be accessed.
- ☐ keep a manual log of Internal access.
- ☐ monitor remote access activities.
- ☒ include a statement in its security policy about Internet use.

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

Question 175

Software quality assurance (QA) reviews are planned as part of system development. At which stage in the development process should the first review be initiated?

- ☐ At pre-implementation planning
- ☐ As a part of the user requirements definition
- ☐ Immediately prior to user acceptance testing
- ☒ During the feasibility study

Question 176

When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

- ☐ Passwords are not shared.
- ☒ Password files are not encrypted.
- ☐ Redundant logon IDs are deleted.
- ☐ The allocation of logon IDs is controlled.

Explanation:

Explanation:

When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon IDs and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

Question 177

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.

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

Question 178

An audit of a database management system found the audit log was not restarted following maintenance. Which of the following is the GREATEST concern to the IS auditor?

- ☒ Changes by the database administrators will not be logged.
- ☐ The database optimization will be compromised.
- ☐ The database triggers and pointers will not be optimized.
- ☐ Changes by application users will not be logged.

Question 179

An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

- ☐ Log all table update transactions.
- ☐ implement before-and-after image reporting.
- ☐ Use tracing and tagging.
- ☒ implement integrity constraints in the database.

Explanation:

Explanation:

Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

Question 180

Key verification is one of the best controls for ensuring that:

- ☒ Data is entered correctly
- ☐ Only authorized cryptographic keys are used
- ☐ Input is authorized
- ☐ Database indexing is performed properly

Explanation:

Explanation:

Key verification is one of the best controls for ensuring that data is entered correctly.

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

Question 181

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 182

Which of the following is a standard secure email protection protocol?

- ☒ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Explanation:

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 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

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

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.

Reference:

CISA review manual 2014 Page number 352 and 353

Question 183

Which of the following is the MOST important outcome of effective risk treatment?

- ☐ Timely reporting of incidents
- ☐ Elimination of risk
- ☒ Implementation of corrective actions
- ☐ Reduced cost of maintaining controls

Question 184

Which of the following concerns is BEST addressed by securing production source libraries?

- ☒ Production source and object libraries may not be synchronized.
- ☐ Unauthorized changes can be moved into production.
- ☐ Programs are not approved before production source libraries are updated.
- ☐ Changes are applied to the wrong version of production source libraries.

Question 185

Which of the following would be considered an essential feature of a network management system?

- ☒ A graphical interface to map the network topology
- ☐ Capacity to interact with the Internet to solve the problems
- ☐ Connectivity to a help desk for advice on difficult issues
- ☐ An export facility for piping data to spreadsheets

Explanation:

Explanation:

To trace the topology of the network, a graphical interface would be essential. It is not necessary that each network be on the internet and connected to a help desk, while the ability to export to a spreadsheet is not an essential element.

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

Question 186

A sender of an e-mail message applies a digital signature to the digest of the message. This action provides assurance of the:

- ☐ date and time stamp of the message.
- ☐ identity of the originating computer.
- ☐ confidentiality of the message's content.
- ☒ authenticity of the sender.

Explanation:

Explanation:

The signature on the digest can be used to authenticate the sender. It does not provide assurance of the date and time stamp or the identity of the originating computer. Digitally signing an e-mail message does not prevent access to its content and, therefore, does not assure confidentiality.

Question 187

Which of the following BEST facilitates compliance with requirements mandating the security of confidential data?

- ☐ Classification of data
- ☐ Security awareness training
- ☒ Encryption of external data transmissions
- ☐ Standardized escalation protocols for breaches

Question 188

Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem?

- ☐ Expert systems
- ☒ Neural networks
- ☐ Integrated synchronized systems
- ☐ Multitasking applications

Explanation:

Explanation:

Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

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

Question 189

The GREATEST benefit of using a maturity model when providing security reports to management is that it presents the:

- ☒ current and target security state for the business.
- ☐ security program priorities to achieve an accepted risk level.
- ☐ assessed level of security risk at a particular point in time.
- ☐ level of compliance with internal policy.

Question 190

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 191

In a public key infrastructure, a registration authority:

- ☒ verifies information supplied by the subject requesting a certificate.
- ☐ issues the certificate after the required attributes are verified and the keys are generated.
- ☐ digitally signs a message to achieve nonrepudiation of the signed message.
- ☐ registers signed messages to protect them from future repudiation.

Explanation:

Explanation:

A registration authority is responsible for verifying information supplied by the subject requesting a certificate, and verifies the requestor's right to request certificate attributes and that the requestor actually possesses the private key corresponding to the public key being sent.

Certification authorities, not registration authorities, actually issue certificates once verification of the information has been completed; because of this, choice B is incorrect. On the other hand, the sender who has control of their private key signs the message, not the registration authority. Registering signed messages is not a task performed by registration authorities.

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

Question 192

Which of the following would BEST enable effective IT resource management?

- ☐ Assessing the risk associated with IT resources
- ☐ Outsourcing IT processes and activities
- ☒ Establishing business priorities
- ☐ Automating business processes

Question 193

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 194

An IS auditor is performing a business continuity plan (BCP) audit and identifies that the plan has not been tested for five years. However, the plan was successfully activated during a recent extended power outage. Which of the following is the IS auditor's BEST course of action?

- ☐ Determine if lessons learned from the activation were incorporated into the plan.
- ☐ Determine if the business impact analysis (BIA) is still accurate.
- ☒ Determine if a follow-up BCP audit is required to identify future gaps.
- ☐ Determine if the annual BCP training program is in need of a review.

Question 195

Test and development environments should be separated. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Test and development environments should be separated, to control the stability of the test environment.

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

Question 196

Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?

- ☐ Reviewing program code
- ☒ Reviewing operations documentation
- ☐ Turning off the UPS, then the power
- ☐ Reviewing program documentation

Explanation:

Explanation:

Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

Question 197

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.

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

Question 198

Which of the following BEST enables system resiliency for an e-commerce organization that requires a low recovery time objective (RTO) and a low recovery point objective (RPO)?

- ☐ Redundant arrays
- ☐ Nightly backups
- ☐ Remote backups
- ☒ Mirrored sites

Question 199

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 200

Which of the following is NOT a defined ISO basic task related to network management?

- ☐ Fault management
- ☐ Accounting resources
- ☐ Security management
- ☒ Communications management

Explanation:

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.

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

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 137).

Question 201

Which of the following factors constitutes a strength in regard to the use of a disaster recovery planning reciprocal agreement?

- ☐ Changes to the hardware or software environment by one company could make the agreement ineffective or obsolete.
- ☐ Reciprocal agreements may not be formally established in a contract.
- ☒ The two companies might share a need for a specialized piece of equipment.
- ☐ A disaster could occur that would affect both companies.

Question 202

Which of the following should an IS auditor expect to see in a network vulnerability assessment?

- ☐ Misconfiguration and missing updates
- ☐ Malicious software and spyware
- ☒ Security design flaws
- ☐ Zero-day vulnerabilities

Question 203

Which of the following is the GREATEST benefit of implementing an incident management process?

- ☐ Opportunity for frequent reassessment of incidents
- ☐ Reduction in security threats
- ☒ Reduction in the business impact of incidents
- ☐ Reduction of costs by the efficient use of resources

Question 204

When reviewing a database supported by a third-party service provider, an IS auditor found minor control deficiencies. The auditor should FIRST discuss recommendations with the:

- ☒ service provider support team manager
- ☐ organization's service level manager
- ☐ organization's chief information officer (CIO)
- ☐ service provider contract liaison

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

Question 205

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- ☐ create the procedures document.
- ☐ terminate the audit.
- ☐ conduct compliance testing.
- ☒ identify and evaluate existing practices.

Explanation:

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

Question 206

The PRIMARY objective of conducting a post-implementation review is to:

- ☐ determine if project management methodology was applied consistently
- ☒ verify that the information system meets the intended objectives
- ☐ determine if testing documentation was sufficient
- ☐ allow employees to provide feedback on the information system

Question 207

During a database audit, an IS auditor noted frequent problems due to the growing size of the order tables. Which of the following is the BEST recommendation in this situation?

- ☒ Develop an archiving approach.
- ☐ Periodically delete completed orders.
- ☐ Build more table indices.
- ☐ Migrate to a different database management system.

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

Question 208

A poor choice of passwords and transmission over unprotected communications lines are examples of:

- ☒ vulnerabilities.
- ☐ threats.
- ☐ probabilities.
- ☐ impacts.

Explanation:

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

Question 209

Machines that operate as a closed system can NEVER be eavesdropped.

- ☐ True
- ☒ False

Explanation:

Explanation:

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

Question 210

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.

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

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

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

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

state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective

nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security

incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take

many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

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

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

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.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

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

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

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

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples belong to corrective control.

Reference:

CISA Review Manual 2014 Page number 44

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

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 211

Which of the following ensures confidentiality of information sent over the internet?

- ☐ Digital signature
- ☐ Digital certificate
- ☐ Online Certificate Status Protocol
- ☒ Private key cryptosystem

Explanation:

Explanation:

Confidentiality is assured by a private key cryptosystem. Digital signatures assure data integrity, authentication and nonrepudiation, but not confidentially. A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity; therefore, it does not address confidentiality. Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of a digital certificate.

Question 212

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:

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 capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

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

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.

The following were incorrect answers:

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

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.

Reference:

CISA review manual 2014 Page number 258

Question 213

Which of the following activities is MOST important in determining whether a test of a disaster recovery plan (DRP) has been successful?

- ☐ Evaluating participation by key personnel
- ☐ Testing at the backup data center
- ☒ Analyzing whether predetermined test objectives were met
- ☐ Testing with offsite backup files

Question 214

An organization is considering moving one of its critical business applications to a cloud hosting service. The cloud provider may not provide the same level of security for this application as the organization. Which of the following will provide the BEST information to help maintain the security posture?

- ☒ Risk assessment
- ☐ Cloud security strategy
- ☐ Vulnerability assessment
- ☐ Risk governance framework

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

Question 215

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

- ☒ translates information security policies and standards into business requirements.
- ☐ articulates management's intent and information security directives in clear language.
- ☐ relates the investment to the organization's strategic plan.
- ☐ realigns information security objectives to organizational strategy.

Question 216

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

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

Question 217

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 218

The MOST effective control to detect fraud inside an organization's network, is to:

- ☐ implement an intrusion detection system (IDS)
- ☐ apply two-factor authentication
- ☒ review access logs
- ☐ segregate duties

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

Question 219

Which of the following is the MOST important issue for an IS auditor to consider with regard to VoIP communications?

- ☐ Continuity of service
- ☐ Homogeneity of the network
- ☐ Nonrepudiation
- ☒ Identity management

Question 220

Which combination of access controls provides the BEST physical protection for a server room?

- ☒ PIN and smart card
- ☐ User ID and PIN
- ☐ Card with a magnetic strip and a smart card
- ☐ Card with a magnetic strip and a shared PIN

Question 221

Which of the following would be MOST useful to an information security manager when conducting a post-incident review of an attack?

- ☐ Details from intrusion detection system logs
- ☒ Method of operation used by the attacker
- ☐ Cost of the attack to the organization
- ☐ Location of the attacker

Question 222

Which of the following is the MOST effective way to achieve the integration of information security governance into corporate governance?

- ☐ Ensure information security aligns with IT strategy.
- ☐ Provide periodic IT balanced scorecards to senior management.
- ☐ Align information security budget requests to organizational goals.
- ☒ Ensure information security efforts support business goals.

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

Question 223

During an audit of a data center, an IS auditor's BEST way to gain an understanding of physical security controls is to:

- ☐ review the data center's physical security procedures.
- ☐ contact the alarm vendor and identify where alarms are installed in the data center.
- ☒ take a tour of the facility and identify physical security controls.
- ☐ obtain the engineering plans for the building and identify points of entry.

Question 224

Which of the following is the MOST significant risk an IS auditor should consider when reviewing a credit card company's application system?

- ☒ Data privacy
- ☐ Processing times
- ☐ System availability
- ☐ Credit ratings

Question 225

While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:

- ☒ shadow file processing.
- ☐ electronic vaulting.
- ☐ hard-disk mirroring.
- ☐ hot-site provisioning.

Explanation:

Explanation:

In shadow file processing, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files, such as airline booking systems. Electronic vaulting electronically transmits data either to direct access storage, an optical disc or another storage medium; this is a method used by banks. Hard-disk mirroring provides redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server. A hot site is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

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

Question 226

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 227

The PRIMARY benefit of integrating information security activities into change management processes is to:

- ☐ protect the organization from unauthorized changes.
- ☒ ensure required controls are included in changes.
- ☐ provide greater accountability for security-related changes in the business.
- ☐ protect the business from collusion and compliance threats.

Question 228

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.

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

Question 229

What influences decisions regarding criticality of assets?

- ☐ The business criticality of the data to be protected
- ☐ Internal corporate politics
- ☒ The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
- ☐ The business impact analysis

Explanation:

Explanation:

Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

Question 230

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 231

You should keep all computer rooms at reasonable humidity levels, which are in between:

- ☒ 20 - 70 percent.
- ☐ 10 - 70 percent.
- ☐ 10 - 60 percent.
- ☐ 70 - 90 percent.
- ☐ 60 - 80 percent.
- ☐ None of the choices.

Explanation:

Explanation:

You should keep all computer rooms at reasonable temperatures, which is in between 60 - 75 degrees Fahrenheit or 10 - 25 degrees Celsius. You should also keep humidity levels at 20 - 70 percent.

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

Question 232

A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ. Which of the following should be evaluated FIRST?

- ☒ Local regulatory requirements
- ☐ Local IT requirements
- ☐ Cross-border data mobility
- ☐ Corporate security objectives

Question 233

An IS auditor discovers that validation controls in a web application have been moved from the server side into the browser to boost performance. This would MOST likely increase the risk of a successful attack by:

- ☐ phishing
- ☒ structured query language (SQL) injection
- ☐ denial of service (DoS)
- ☐ buffer overflow

Question 234

Which of the following presents the GREATEST concern when implementing data flow across borders?

- ☐ Software piracy laws
- ☒ National privacy laws
- ☐ Political unrest
- ☐ Equipment incompatibilities

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

Question 235

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 236

Organizations should use off-site storage facilities to maintain _____ (fill in the blank) of current and critical information within backup files.

- ☐ Confidentiality
- ☐ Integrity
- ☒ Redundancy
- ☐ Concurrency

Explanation:

Explanation:

Redundancy is the best answer because it provides both integrity and availability. Organizations should use off-site storage facilities to maintain redundancy of current and critical information within backup files.

Question 237

Which of the following tools BEST demonstrate the effectiveness of the information security program?

- ☒ A security balanced scorecard
- ☐ Management satisfaction surveys
- ☐ Risk heat map
- ☐ Key risk indicators (KRIs)

Question 238

Which of the following is MOST important to include in an organization's incident response plan to help prevent similar incidents from happening in the future?

- ☐ Documentation of incident details
- ☐ Incident closure procedures
- ☐ Containment and neutralization actions
- ☒ Post-incident review

Question 239

An IS auditor reviewing a new application for compliance with information privacy principles should be the MOST concerned with:

- ☐ nonrepudiation
- ☒ collection limitation
- ☐ availability
- ☐ awareness

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

Question 240

What is the MOST difficult aspect of access control in a multiplatform, multiple-site client/server environment?

- ☐ Creating new user IDs valid only on a few hosts
- ☒ Maintaining consistency throughout all platforms
- ☐ Restricting a local user to necessary resources on a local platform
- ☐ Restricting a local user to necessary resources on the host server

Question 241

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 242

In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

- ☐ connectionless integrity.
- ☐ data origin authentication.
- ☐ antireplay service.
- ☒ confidentiality.

Explanation:

Explanation:

Both protocols support choices A, B and C, but only the ESP protocol provides confidentiality via encryption.

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

Question 243

Which of the following will enable a customer to authenticate an online Internet vendor?

- ☐ Vendor signs a reply using a hash function and the customer's public key.
- ☐ Customer encrypts an order using the vendor's public key.
- ☒ Customer verifies the vendor's certificate with a certificate authority (CA).
- ☐ Vendor decrypts incoming orders using its own private key.

Question 244

Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

- ☐ Change management
- ☐ Backup and recovery
- ☐ incident management
- ☒ Configuration management

Explanation:

Explanation:

The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new release fail, the baseline will provide a point to which to return. The other choices do not provide the processes necessary for establishing software release baselines and are not related to software release baselines.

Question 245

Documentation of a business case used in an IT development project should be retained until:

- ☒ the end of the system's life cycle.
- ☐ the project is approved.
- ☐ user acceptance of the system.
- ☐ the system is in production.

Explanation:

Explanation:

A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates vs. actuals. Questions like, 'why do we do that', 'What was the original intent' and 'how did we perform against the plan' can be answered, and lessons for developing future business cases can be learned. During the development phase of a project one should always validate the business case, as it is a good management instrument. After finishing a project and entering production, the business case and all the completed research are valuable sources of information that should be kept for further reference

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

Question 246

Which of the following is the BEST reason for delaying the application of a critical security patch?

- ☐ Lack of vulnerability management
- ☐ Conflicts with software development life cycle
- ☒ Technology interdependencies
- ☐ Resource limitations

Question 247

Which of the following is the MOST appropriate document for granting authority to an external IS auditor in an audit engagement with a client organization?

- ☒ Approved statement of work
- ☐ Formally approved audit charter
- ☐ An internal memo to all concerned parties
- ☐ Request for proposal for audit services

Question 248

The final decision to include a material finding in an audit report should be made by the:

- ☐ audit committee.
- ☐ auditee's manager.
- ☒ IS auditor.
- ☐ CEO of the organization

Explanation:

Explanation:

The IS auditor should make the final decision about what to include or exclude from the audit report. The other choices would limit the independence of the auditor.

Question 249

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

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

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

Question 250

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 251

Which of the following is a step in establishing a security policy?

- ☐ Developing platform-level security baselines.
- ☐ Developing configurations parameters for the network,
- ☒ Implementing a process for developing and maintaining the policy.
- ☐ Creating a RACI matrix.

Question 252

In an organization where IT is critical to its business strategy and where there is a high level of operational dependence on IT, senior management commitment to security is BEST demonstrated by the:

- ☐ reporting line of the chief information security officer (CISO).
- ☐ segregation of duties policy.
- ☒ existence of an IT steering committee.
- ☐ size of the IT security function.

Question 253

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 254

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 255

Which of the following is the BEST indication that an organization's vulnerability identification capability has achieved a high level of maturity?

- ☐ The organization collaborates with relevant partners to correlate vulnerability data.
- ☐ Known application vulnerabilities are manually categorized and prioritized.
- ☐ Vulnerability management tools are tailored for specific operating systems.
- ☒ Tools are in place to periodically identity new and updated vulnerabilities.

Question 256

A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?

- ☐ Comparing source code
- ☒ Reviewing system log files
- ☐ Comparing object code
- ☐ Reviewing executable and source code integrity

Explanation:

Explanation:

Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library. Source and object code comparisons are ineffective, because the original programs were restored and do not exist. Reviewing executable and source code integrity is an ineffective control, because integrity between the executable and source code is automatically maintained.

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

Question 257

An organization has selected a web-based solution to reduce transaction costs and improve productivity. Before implementation, an IS auditor should ensure that the organization has:

- ☐ performed a vulnerability assessment.
- ☐ implemented electronic data interchange.
- ☐ validated the solution against the current IT infrastructure.
- ☒ addressed the level of risk exposure.

Question 258

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 259

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.

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

Question 260

When an intrusion into an organization's network is detected, which of the following should be performed FIRST?

- ☐ Block all compromised network nodes.
- ☐ Protect information in the compromised systems.
- ☒ Develop a response to the incident.
- ☐ Identify nodes that have been compromised.

Question 261

A certificate authority (CA) can delegate the processes of:

- ☐ revocation and suspension of a subscriber's certificate.
- ☐ generation and distribution of the CA public key.
- ☒ establishing a link between the requesting entity and its public key.
- ☐ issuing and distributing subscriber certificates.,

Explanation:

Explanation:

Establishing a link between the requesting entity and its public key is a function of a registration authority. This may or may not be performed by a CA; therefore, this function can be delegated. Revocation and suspension and issuance and distribution of the subscriber certificate are functions of the subscriber certificate life cycle management, which the CA must perform.

Generation and distribution of the CA public key is a part of the CA key life cycle management process and, as such, cannot be delegated.

Question 262

An IS auditor finds that the cost of developing an application is now projected to significantly exceed the budget. Which of the following is the GREATEST risk to communicate to senior management?

- ☐ Increased staff turnover
- ☒ Project abandonment
- ☐ Noncompliance with project methodology
- ☐ Inability to achieve expected benefits

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

Question 263

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 264

A region where an organization conducts business has announced changes in privacy legislation. Which of the following should an IS auditor do FIRST to prepare for the changes?

- ☒ Perform a gap analysis with current privacy procedures.
- ☐ Provide suggested updates to the organization's privacy procedures.
- ☐ Communicate the changes in privacy legislation to the legal department.
- ☐ Design compensating controls to be in compliance with new privacy legislation.

Question 265

What are the different types of Audits?

- ☒ Compliance, financial, operational, forensic and integrated
- ☐ Compliance, financial, operational, G9 and integrated
- ☐ Compliance, financial, SA1, forensic and integrated
- ☐ Compliance, financial, operational, forensic and capability

Explanation:

Explanation:

Compliance, financial, operational, forensic and integrated are different types of audit.

For your exam you should know the information below:

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

What is an audit?

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

Compliance Audit

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

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

Financial Audit

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

Operational Audit

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

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

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

Objectives

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

To understand the responsibilities and risks faced by an organization.

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

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

Integrated Audits

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

IS Audit

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

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

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

Forensic Audit

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

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

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

The following answers are incorrect:

Compliance, financial, operational, forensic and integrated are different types of audits. G9, SA1 and capability are not the audit types.

Reference:

CISA Review Manual 2014 Page number 47

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

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

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

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

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

Question 266

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

- ☒ Traffic analysis
- ☐ SYN flood
- ☐ Denial of service (DoS)
- ☐ Distributed denial of service (DoS)

Explanation:

Explanation:

Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

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

Question 267

When reviewing capacity monitoring, an IS auditor notices several incidents where storage capacity limits were reached, while the average utilization was below 30%. Which of the following would the IS auditor MOST likely identify as the root cause?

- ☐ The IT response to the alerts was too slow.
- ☐ The amount of data produced was unacceptable for operations.
- ☐ The storage space should have been enlarged in time.
- ☒ The dynamics of the utilization were not properly taken into account.

Question 268

An employee who denies accusations of sending inappropriate images to other employees has been discharged. For evidential purposes, the mail database for the discharged employee's computer should be:

- ☐ deleted as it could subject the organization to further legal liability
- ☐ impounded by physically removing the disk drive
- ☒ backed up to the server, where its access can be tightly restricted
- ☐ copied to write-once, read-many media using the computer's OS tools

Question 269

Which of the following is the BEST source of information for assessing the effectiveness of IT process monitoring?

- ☐ Participative management techniques
- ☐ Quality assurance (QA) reviews
- ☐ Performance data
- ☒ Real-time audit software

Question 270

An IS auditor determines that a business impact analysis (BIA) was not conducted during the development of a business continuity plan (BCP). What is the MOST significant risk that could result from this situation?

- ☐ Responsibilities are not property defined.
- ☐ Recovery time objectives (RTOs) are not correctly determined.
- ☐ Key performance indicators (KPIs) are not aligned.
- ☒ Critical business applications are not covered.

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

Question 271

A decision support system (DSS):

- ☐ is aimed at solving highly structured problems.
- ☐ combines the use of models with nontraditional data access and retrieval functions.
- ☒ emphasizes flexibility in the decision making approach of users.
- ☐ supports only structured decision making tasks.

Explanation:

Explanation:

DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semi structured decision making tasks.

Question 272

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 273

Which of the following would be the GREATEST concern to an IS auditor reviewing an IT outsourcing arrangement?

- ☒ Several IT personnel perform the same functions as the vendor.
- ☐ The contract does not include a renewal option.
- ☐ Development of KPIs that will be used was assigned to the vendor.
- ☐ Some penalties were waived during contract negotiations.

Question 274

An organization plans to implement a virtualization strategy enabling multiple operating systems on a single host. Which of the following should be the GREATEST concern with this strategy?

- ☐ Adequate storage space
- ☐ Complexity of administration
- ☐ Network bandwidth
- ☒ Application performance

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

Question 275

Since data storage of a critical business application is on a redundant array of inexpensive disks (RAID), backups are not considered essential. The IS auditor should recommend proper backups because RAID:

- ☐ relies on proper maintenance.
- ☐ cannot offer protection against disk corruption.
- ☒ cannot recover from a natural disaster.
- ☐ disks cannot be hot-swapped for quick recovery.

Question 276

The MOST likely explanation for the use of applets in an Internet application is that:

- ☐ it is sent over the network from the server.
- ☐ the server does not run the program and the output is not sent over the network.
- ☒ they improve the performance of the web server and network.
- ☐ it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Explanation:

Explanation:

An applet is a JAVA program that is sent over the network from the web server, through a web browser and to the client machine; the code is then run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network-over which the server and client are connected-drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

Question 277

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 278

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:

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:

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

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 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.

Reference:

CISA review manual 2014 Page number 350 and 351

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

Question 279

Which of the following is BEST addressed when using a timestamp within a digital signature to deliver sensitive financial information?

- ☒ Replay protection
- ☐ Authentication
- ☐ Nonrepudiation
- ☐ Data integrity

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

Question 280

IT service engineers at a large organization are unable to effectively prioritize system-generated alerts from hundreds of applications running across multiple servers and databases. As a result, many alerts are often ignored, leading to major problems including downtime. Which of the following is the BEST IS audit recommendation to address this situation?

- ☐ Prioritize alerts from legacy applications that may require remote support from external vendors.
- ☐ Implement a threshold management system that prioritizes alerts over a certain age.
- ☐ Develop a classification scheme that prioritizes alerts according to potential business impact.
- ☒ Group alerts from related systems and immediately escalate to the application owner.

Question 281

Which of the following is the PRIMARY purpose of red team testing?

- ☒ To determine the organization's preparedness for an attack
- ☐ To confirm the risk profile of the organization
- ☐ To assess the vulnerability of employees to social engineering
- ☐ To establish a baseline incident response program

Question 282

After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?

- ☒ Perform an integral review of the recovery tasks.
- ☐ Broaden the processing capacity to gain recovery time.
- ☐ Make improvements in the facility's circulation structure.
- ☐ increase the amount of human resources involved in the recovery.

Explanation:

Explanation:

Performing an exhaustive review of the recovery tasks would be appropriate to identify the way these tasks were performed, identify the time allocated to each of the steps required to accomplish recovery, and determine where adjustments can be made. Choices B, C and D could be actions after the described review has been completed.

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

Question 283

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 284

A structured walk-through test of a disaster recovery plan involves:

- ☐ representatives from each of the functional areas coming together to go over the plan.
- ☒ all employees who participate in the day-to-day operations coming together to practice executing the plan.
- ☐ moving the systems to the alternate processing site and performing processing operations.
- ☐ distributing copies of the plan to the various functional areas for review.

Explanation:

Explanation:

A structured walk-through test of a disaster recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required. Choice B is a simulation test to prepare and train the personnel who will be required to respond to disasters and disruptions. Choice C is a form of parallel testing to ensure that critical systems will perform satisfactorily in the alternate site. Choice D is a checklist test.

Question 285

An IS auditor finds that an organization's data loss prevention (DLP) system is configured to use vendor default settings to identify violations. The auditor's MAIN concern should be that:

- ☒ violations may not be categorized according to the organization's risk profile.
- ☐ violation reports may not be retained according to the organization's risk profile.
- ☐ violation reports may not be reviewed in a timely manner.
- ☐ a significant number of false positive violations may be reported.

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

Question 286

A finance department director has decided to outsource the organization's budget application and has identified potential providers. Which of the following actions should be initiated FIRST by the information security manager?

- ☐ Validate that connectivity to the service provider can be made securely.
- ☒ Obtain audit reports on the service providers hosting environment.
- ☐ Review the disaster recovery plans (DRP) of the providers.
- ☐ Align the roles of the organization's and the service providers' staffs.

Question 287

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

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

Explanation:

Explanation:

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

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

Question 288

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

- ☐ ask the auditee to sign a release form accepting full legal responsibility.
- ☒ elaborate on the significance of the finding and the risks of not correcting it.
- ☐ report the disagreement to the audit committee for resolution.
- ☐ accept the auditee's position since they are the process owners.

Explanation:

Explanation:

If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

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

Question 289

Input/output controls should be implemented for which applications in an integrated systems environment?

- ☐ The receiving application
- ☐ The sending application
- ☒ Both the sending and receiving applications
- ☐ Output on the sending application and input on the receiving application

Explanation:

Explanation:

Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

Question 290

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 291

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 292

The MOST important reason to use a centralized mechanism to identify information security incidents is to:

- ☐ prevent unauthorized changes to networks.
- ☐ comply with corporate policies.
- ☐ detect potential fraud.
- ☒ detect threats across environments.

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

Question 293

A vulnerability in which of the following virtual systems should be of GREATEST concern to an IS auditor?

- ☒ The virtual machine management server
- ☐ The virtual application server
- ☐ The virtual antivirus server
- ☐ The virtual file server

Question 294

Which of the following provides the BEST assurance that security policies are applied across business operations?

- ☐ Organizational standards are required to be formally accepted.
- ☐ Organizational standards are enforced by technical controls.
- ☐ Organizational standards are included in awareness training.
- ☒ Organizational standards are documented in operational procedures.

Question 295

An IS auditor would MOST likely recommend that IT management use a balanced scorecard to:

- ☐ ensure that IT staff meet performance requirements.
- ☐ train and educate IT staff.
- ☐ indicate whether the organization meets quality standards.
- ☒ assess IT functions and processes.

Question 296

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 297

Which of the following is MOST directly affected by network performance monitoring tools?

- ☐ Integrity
- ☒ Availability
- ☐ Completeness
- ☐ Confidentiality

Explanation:

Explanation:

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

Question 298

Which of the following would MOST effectively minimize the risk of unauthorized online banking customer transactions due to phishing?

- ☐ A strong authentication mechanism
- ☐ Clear audit trails
- ☐ An intrusion prevention system (IPS)
- ☒ A customer awareness program

Question 299

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- ☒ sufficient evidence will be collected.
- ☐ all significant deficiencies identified will be corrected within a reasonable period.
- ☐ all material weaknesses will be identified.
- ☐ audit costs will be kept at a minimum level.

Explanation:

Explanation:

Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of

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

professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

Question 300

Which of the following BEST ensures the integrity of a server's operating system?

- ☐ Protecting the server in a secure location
- ☐ Setting a boot password
- ☒ Hardening the server configuration
- ☐ Implementing activity logging

Explanation:

Explanation:

Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario-it is a detective control (not a preventive one), and the attacker who already gained privileged access can modify logs or disable them.

Question 301

Which of the following is the GREATEST cause for concern when an organization is planning to migrate business-critical applications to the cloud using a Platform as a Service (PaaS) model?

- ☒ The organization will not manage operating system patches.
- ☐ The cloud provider does not offer regional redundancy.
- ☐ Compliance requirements are not being validated.
- ☐ Application data will not be encrypted at rest.

Question 302

Which of the following function in traditional EDI process manipulates and routes data between the application system and the communication handler?

- ☐ Communication handler
- ☒ EDI Interface
- ☐ Application System
- ☐ EDI Translator

Explanation:

Explanation:

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

EDI Interface manipulates and routes data between the application system and the communication handler.

For your exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's computer system

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox services similar to post offices. The VAN receives all the outbound transactions from an organization, sort them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

EDI Interface – Interface function that manipulates and routes data between the application system and the communication handler. The interface consists of two components

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping. Data mapping is the process by which data are extracted from EDI translation process and integrated with the data or process of receiving company.

3. Application System – The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN).

Application System – The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

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

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Reference:

CISA review manual 2014 Page number 178

Question 303

An IS auditor is reviewing database log settings and notices that only INSERT and DELETE operations are being monitored in the database. What is the MOST significant risk?

- ☐ Metadata may not be logged
- ☒ Newly added records may not be logged
- ☐ Purged records may not be logged
- ☐ Changes to existing records may not be logged

Question 304

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:

Explanation:

There are 4 major considerations in the chain of event in regards to evidence in computer forensics:

Identify -Refers to identification of information that is available and might form evidence of an accident

Preserve -Refers to the practice of retrieving identified information and preserving it as evidence. The practice generally includes the imaging of original media in presence of an independent third party. The process also requires being able to document chain-of-custody so that it can be established in a court law.

Analyze – Involves extracting, processing and interpreting the evidence. Extracted data could be unintelligible binary data after it has been processed and converted into human readable format.

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

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.

Reference:

CISA review manual 2014 Page number367

Question 305

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

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

Question 306

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.

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

Question 307

Which of the following is the BEST key performance indicator (KPI) for determining how well the IT policy is aligned to the business requirements?

- ☒ Number of approved exceptions to the policy
- ☐ Total cost of policy breaches
- ☐ Total cost to support the policy
- ☐ Number of inquiries regarding the policy

Question 308

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 309

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:

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

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 310

Two organizations will share ownership of a new enterprise resource management (ERM) system. To help ensure the successful implementation of the system, it is MOST important to define:

- ☒ access to data
- ☐ the governance model
- ☐ custody of assets
- ☐ appropriate procedures

Question 311

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

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

access is important, but it is only a detective control that will not provide adequate protection to sensitive information.

Question 312

An IS auditor is performing a follow-up audit for findings identified in an organization's user provisioning process. Which of the following is the MOST appropriate population to sample from when testing for remediation?

- ☐ All users who have followed user provisioning processes provided by management
- ☐ All users provisioned after the finding was originally identified
- ☒ All users provisioned after management resolved the audit issue
- ☐ All users provisioned after the final audit report was issued

Question 313

Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

Question 314

An organization that has suffered a cyber attack is performing a forensic analysis of the affected users' computers. Which of the following should be of GREATEST concern for the IS auditor reviewing this process?

- ☒ The chain of custody has not been documented.
- ☐ The legal department has not been engaged.
- ☐ An imagining process was used to obtain a copy of the data from each computer.
- ☐ Audit was only involved during extraction of the information.

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

Question 315

A PRIMARY advantage of involving business management in evaluating and managing information security risks is that they:

- ☐ better understand the security architecture
- ☐ better understand organizational risks
- ☒ can balance technical and business risks
- ☐ are more objective than security management

Question 316

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:

Explanation:

ECC demands less computational power and, therefore offers more security per bit. For example, an ECC with a 160-bit key offer the same security as an RSA based system with a 1024-bit key.

ECC is a variant and more efficient form of a public key cryptography (how tom manage more security out of minimum resources) gaining prominence is the ECC. ECC works well on a network computer requires strong cryptography but have some limitation such as bandwidth and processing power. This is even more important with devices such as smart cards, wireless phones and other mobile devices.

The following were incorrect answers:

Quantum Cryptography - Quantum cryptography is based on a practical application of the characteristics of the smallest “grain” of light, photons and on physical laws governing their generation, propagation and detection. Quantum cryptography is the next generation of cryptography that may solve some of the existing problem associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys. Initial commercial usage has already started now that the laboratory research phase has been completed.

Symmetric Encryption - Symmetric encryption is the oldest and best-known technique. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This might be as simple as shifting each letter by a number

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

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.

Reference:

CISA review manual 2014 Page number 349 and 350

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

Question 317

An organization plans to deploy Wi-Fi location analytics to count the number of shoppers per day across its various retail outlets. What should the IS auditor recommend as the FIRST course of action by IT management?

- ☒ Conduct a privacy impact assessment
- ☐ Mask media access control (MAC) addresses
- ☐ Survey shoppers for feedback
- ☐ Develop a privacy notice to be displayed to shoppers

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

Question 318

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:

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.

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

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 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.

Reference:

CISA review manual 2014 Page number 183

Question 319

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 320

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

- ☐ Observe the response mechanism.
- ☐ Clear the virus from the network.
- ☒ Inform appropriate personnel immediately.
- ☐ Ensure deletion of the virus.

Explanation:

Explanation:

The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response. Choice A should be taken after choice

C. This will enable an IS auditor to examine the actual workability and effectiveness of the response system. An IS auditor should not make changes to the system being audited, and ensuring the deletion of the virus is a management responsibility.

Question 321

The drives of a tile server are backed up at a hot site. Which of the following is the BEST way to duplicate the files stored on the server for forensic analysis?

- ☒ Capture a bit-by-bit image of the file server's drives.
- ☐ Run forensic analysis software on the backup drive.
- ☐ Create a logical copy of the file server's drives.
- ☐ Replicate the server's volatile data to another drive.

Question 322

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 323

An IS audit concludes that entry to the computer room is appropriately controlled. The audit result provides assurance that:

- ☐ the theft of hardware is prevented.
- ☐ the confidentiality of data is protected.
- ☐ data leakage is prevented.
- ☒ unauthorized access is prevented.

Question 324

To support an organization's goals, an IS department should have:

- ☐ a low-cost philosophy.
- ☒ long- and short-range plans.
- ☐ leading-edge technology.
- ☐ plans to acquire new hardware and software.

Explanation:

Explanation:

To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

Question 325

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

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

Explanation:

Explanation:

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

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

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

Question 326

An IS auditor should expect the responsibility for authorizing access rights to production data and systems to be entrusted to the:

- ☐ process owners.
- ☐ system administrators.
- ☐ security administrator.
- ☒ data owners.

Explanation:

Explanation:

Data owners are primarily responsible for safeguarding the data and authorizing access to production data on a need-to-know basis.

Question 327

As part of a quality assurance initiative, an organization has engaged an external auditor to evaluate the internal IS audit function. Which of the following observations should be of MOST concern?

- ☐ Audit reports are not approved by the audit committee.
- ☒ Audit reports do not state they are conducted in accordance with industry standards.
- ☐ The audit team is not sufficiently leveraging data analytics.
- ☐ Audit engagements are not risk-based.

Question 328

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.

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

Question 329

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 330

When reviewing a hardware maintenance program, an IS auditor should assess whether:

- ☐ the schedule of all unplanned maintenance is maintained.
- ☐ it is in line with historical trends.
- ☐ it has been approved by the IS steering committee.
- ☒ the program is validated against vendor specifications.

Explanation:

Explanation:

Though maintenance requirements vary based on complexity and performance workloads, a hardware maintenance schedule should be validated against the vendor-provided specifications. For business reasons, an organization may choose a more aggressive maintenance program than the vendor's program. The maintenance program should include maintenance performance history, be it planned, unplanned, executed or exceptional. Unplanned maintenance cannot be scheduled. Hardware maintenance programs do not necessarily need to be in line with historical trends. Maintenance schedules normally are not approved by the steering committee.

Question 331

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 332

Total billing amounts on invoices are automatically transferred to an organization's account ledger weekly. During an IS audit, the auditor discovers that one week's billing is missing from the ledger. Which of the following areas should the auditor examine FIRST?

- ☐ Annual reconciliations
- ☐ Change management
- ☒ Batch processing controls
- ☐ Module access rights

Question 333

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- ☒ improve internal control procedures.
- ☐ harden the network to industry best practices.
- ☐ highlight the importance of incident response management to management.
- ☐ improve employee awareness of the incident response process.

Explanation:

Explanation:

A postincident review examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls. Understanding the purpose and structure of postincident reviews and follow-up procedures enables the information security manager to continuously improve the security program. Improving the incident response plan based on the incident review is an internal (corrective) control. The network may already be hardened to industry best practices. Additionally, the network may not be the source of the incident. The primary objective is to improve internal control procedures, not to highlight the importance of incident response management (IRM), and an incident response (IR) review does not improve employee awareness.

Question 334

Which of the following BEST enables effective closure of noncompliance issues?

- ☐ Insuring against the risk
- ☐ Performing control self-assessments
- ☒ Capturing issues in a risk register
- ☐ Executing an approved mitigation plan

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

Question 335

What is the BEST approach to mitigate the risk of a phishing attack?

- ☐ implement an intrusion detection system (IDS)
- ☐ Assess web site security
- ☐ Strong authentication
- ☒ User education

Explanation:

Explanation:

Phishing attacks can be mounted in various ways; intrusion detection systems (IDSs) and strong authentication cannot mitigate most types of phishing attacks. Assessing web site security does not mitigate the risk. Phishing uses a server masquerading as a legitimate server. The best way to mitigate the risk of phishing is to educate users to take caution with suspicious internet communications and not to trust them until verified. Users require adequate training to recognize suspicious web pages and e-mail.

Question 336

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- ☐ Function point analysis
- ☒ PERT chart
- ☐ Rapid application development
- ☐ Object-oriented system development

Explanation:

Explanation:

A PERT chart will help determine project duration once all the activities and the work involved with those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

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

Question 337

Which of the following will BEST protect an organization against spear phishing?

- ☐ Email content filtering
- ☐ Acceptable use policy
- ☒ End-user training
- ☐ Antivirus software

Question 338

Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?

- ☐ Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
- ☐ During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
- ☐ The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
- ☒ Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Explanation:

Explanation:

A disaster recovery test should test the plan, processes, people and IT systems. Therefore, if the plan is not used, its accuracy and adequacy cannot be verified. Disaster recovery should not rely on key staff since a disaster can occur when they are not available. It is common that not all systems can be tested in a limited test time frame. It is important, however, that those systems which are essential to the business are tested, and that the other systems are eventually tested throughout the year. One aim of the test is to identify and replace defective devices so that all systems can be replaced in the case of a disaster. Choice B would only be a concern if the number of discovered problems is systematically very high, in a real disaster, there is no need for a clean shutdown of the original production environment since the first priority is to bring the backup site up.

Question 339

Based on the guidance of internal audit, an IT steering committee is considering the use of a balanced scorecard to evaluate its project management process. Which of the following is the GREATEST advantage to using this approach?

- ☐ Project schedule and budget management will improve.
- ☒ Performance is measured from different perspectives.
- ☐ Information is provided in a consistent and timely manner.
- ☐ Project will be prioritized based on value.

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

Question 340

Which of the following is the MOST reliable sender authentication method?

- ☐ Digital signatures
- ☐ Asymmetric cryptography
- ☒ Digital certificates
- ☐ Message authentication code

Explanation:

Explanation:

Digital certificates are issued by a trusted third party. The message sender attaches the certificate and the recipient can verify authenticity with the certificate repository. Asymmetric cryptography, such as public key infrastructure (PKI), appears to authenticate the sender but is vulnerable to a man-in-the-middle attack. Digital signatures are used for both authentication and confidentiality, but the identity of the sender would still be confirmed by the digital certificate. Message authentication code is used for message integrity verification.

Question 341

An internal audit department recently established a quality assurance (QA) program. Which of the following activities is MOST important to include as part of the QA program requirements?

- ☒ Ongoing monitoring of the audit activities
- ☐ Analysis of user satisfaction reports from business lines.
- ☐ Feedback from internal audit staff
- ☐ Long-term internal audit resource planning

Question 342

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:

Explanation:

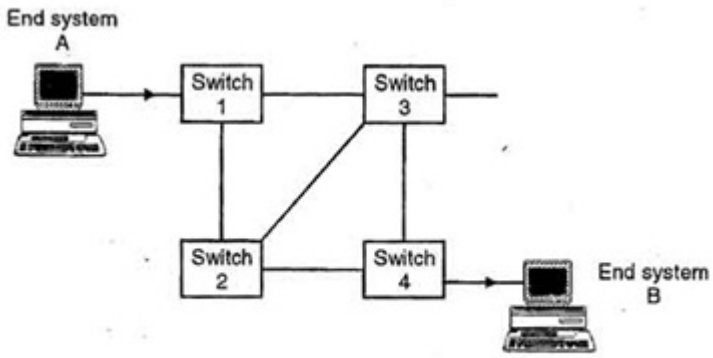
For your exam you should know below information about WAN message transmission technique:

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

Message Switching

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

Message Switching



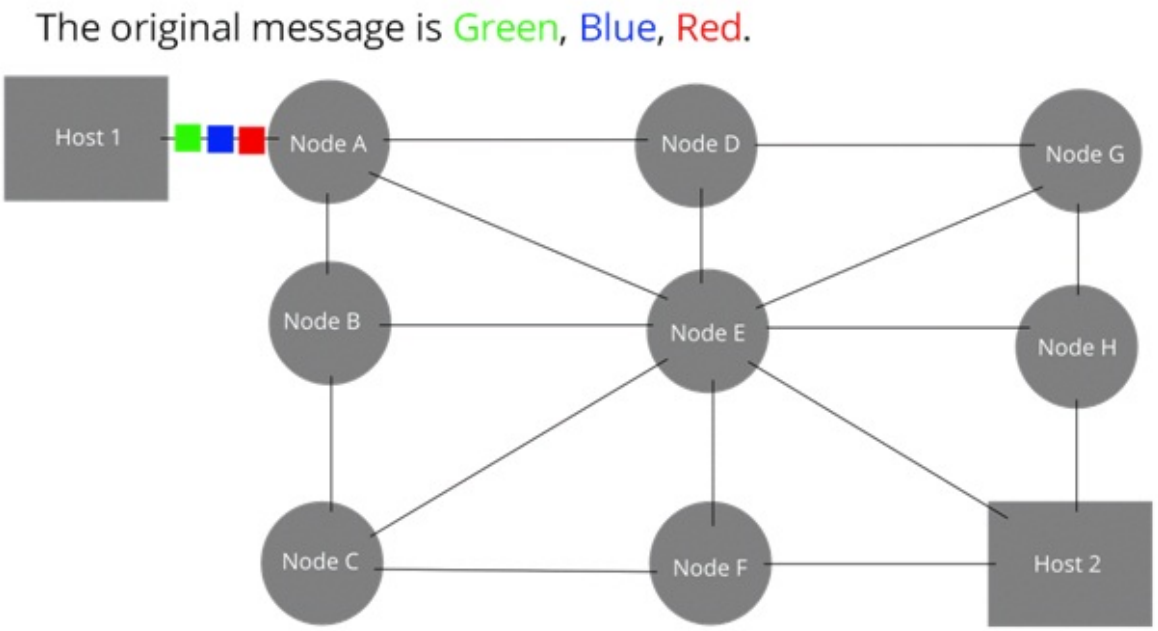
Message switched data network

Packet Switching

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

Packet Switching

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



Circuit Switching

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

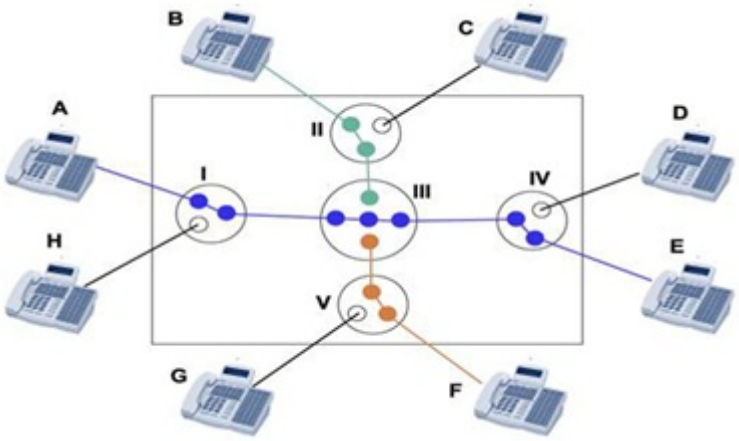
The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the session. The circuit functions as if the nodes were physically connected similar to an electrical circuit.

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

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

Circuit Switching

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



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

Difference between Circuit and packet switching

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

Virtual circuit

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

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

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.

Reference:

CISA review manual 2014 Page number 265

Question 343

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 344

During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall. Which of the following controls has MOST likely been compromised?

- ☐ Identification
- ☐ Data integrity
- ☐ Data validation
- ☒ Authentication

Question 345

An audit of the quality management system (QMS) begins with an evaluation of the:

- ☒ organization's QMS policy
- ☐ sequence and interaction of QMS processes
- ☐ QMS processes and their application
- ☐ QMS document control procedures

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

Question 346

An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

Question 347

Which of the following features can be provided only by asymmetric encryption?

- ☐ 128-bit key length
- ☐ Information privacy
- ☒ Data confidentiality
- ☐ Nonrepudiation

Question 348

Which of the following is the MOST effective way to identify anomalous transactions when performing a payroll fraud audit?

- ☐ Substantive testing of payroll files
- ☒ Data analytics on payroll data
- ☐ Observation of payment processing
- ☐ Sample-based review of pay stubs

Question 349

An external security audit risk has reported multiple instances of control noncompliance. Which of the following would be MOSTimportant for the information security manager to communicate to senior management?

- ☒ The impact of noncompliance on the organization's risk profile
- ☐ An accountability report to initiate remediation activities
- ☐ A plan for mitigating the risk due to noncompliance
- ☐ Control owner responses based on a root cause analysis

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

Question 350

Which of the following process consist of identification and selection of data from the imaged data set in computer forensics?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☒ Extraction

Explanation:

Explanation:

Extraction is the process of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

For CISA exam you should know below mentioned key elements of computer forensics during audit planning.

Data Protection -To prevent sought-after information from being altered, all measures must be in place. It is important to establish specific protocol to inform appropriate parties that electronic evidence will be sought and not destroy it by any means.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device 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:

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Reporting -The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis.

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

Explanation:

CISA review manual 2014 Page number 367 and 368

Question 351

Which of the following access control situations represents the MOST serious control weakness?

- ☐ Computer operators have access to system level flowcharts.
- ☐ Programmers have access to development hardware.
- ☒ End users have access to program development tools.
- ☐ System developers have access to production data.

Question 352

Which of the following would be MOST critical for an IS auditor to look for when evaluating fire precautions in a manned data center located in the upper floor of a multi-story building?

- ☐ Existence of handheld fire extinguishers in highly visible locations
- ☐ Documentation of regular inspections by the local fire department
- ☐ Adequacy of the HVAC system throughout the facility
- ☒ Documentation of tested emergency evacuation plans

Question 353

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 354

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organization's information security manager?

- ☐ The operations team implemented the change without regression testing.
- ☒ The change did not include a proper assessment of risk.
- ☐ Documentation of the change was made after implementation.
- ☐ The information security manager did not review the change prior to implementation.

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

Question 355

At a project steering committee meeting, it is stated that adding controls to business processes undergoing re-engineering is an unnecessary cost. The IS auditor's BEST response is that the actual control overhead for a business process is:

- ☐ usually considerable, but the benefits of good controls always exceed the cost.
- ☐ the responsibility of the project manager, and the cost should have been included in the budget.
- ☐ usually difficult to ascertain but is justifiable, because controls are essential to doing business
- ☒ usually less than the potential cost of failure caused by lack of controls.

Question 356

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 357

An organization's data retention policy states that all data will be backed up, retained for 10 years, and then destroyed. When conducting an audit of the long-term offsite backup program, an IS auditor should:

- ☐ verify that business owners review data before it is destroyed.
- ☒ verify that there is a process to ensure readability and restore capability.
- ☐ confirm that business interruption insurance coverage is in place.
- ☐ review data classification schemes for appropriate security levels.

Question 358

Rather than decommission an entire legacy application, an organization's IT department has chosen to replace specific modules while maintaining those still relevant. Which of the following artifacts is MOST important for an IS auditor to review?

- ☐ IT service management catalog and service level requirements
- ☐ Security requirements for legacy data masking and data destruction
- ☐ Applicable licensing agreements for the application
- ☒ Future state architecture and requirements

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

Question 359

Network ILD&P are typically installed:

- ☐ on the organization's internal network connection.
- ☒ on the organization's internet network connection.
- ☐ on each end user stations.
- ☐ on the firewall.
- ☐ None of the choices.

Explanation:

Explanation:

Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

Question 360

Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities BEST supports the concept of integrity?

- ☐ Ensuring encryption for data in transit
- ☐ Implementing a data classification schema
- ☒ Utilizing a formal change management process
- ☐ Enforcing service level agreements (SLAs)

Question 361

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

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

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.

Question 362

How is the risk of improper file access affected upon implementing a database system?

- ☐ Risk varies.
- ☐ Risk is reduced.
- ☐ Risk is not affected.
- ☒ Risk is increased.

Explanation:

Explanation:

Improper file access becomes a greater risk when implementing a database system.

Question 363

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

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

Question 364

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 365

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:

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

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.

Question 366

An IS auditor is reviewing an organization's primary router access control list. Which of the following should result in a finding?

- ☐ The network security group can change network address translation (NAT).
- ☐ There are conflicting permit and deny rules for the IT group.
- ☐ There is only one rule per group with access privileges.
- ☒ Individual permissions are overriding group permissions.

Question 367

Naming conventions for system resources are important for access control because they:

- ☐ ensure that resource names are not ambiguous.
- ☒ reduce the number of rules required to adequately protect resources.
- ☐ ensure that user access to resources is clearly and uniquely identified.
- ☐ ensure that internationally recognized names are used to protect resources.

Explanation:

Explanation: Naming conventions for system resources are important for the efficient administration of security controls. The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

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

Question 368

Which of the following ACID property in DBMS means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☒ Durability

Explanation:

Explanation:

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction. [citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

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

The following were incorrect answers:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

Reference:

CISA review manual 2014 Page number 218

Question 369

Which of the following provides the GREATEST assurance that an organization allocates appropriate resources to respond to information security events?

- ☐ Incident classification procedures
- ☐ Threat analysis and intelligence reports
- ☒ An approved IT staffing plan
- ☐ Information security policies and standards.

Question 370

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

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

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

Question 371

Which of the following should the IS auditor do FIRST to ensure data transfer integrity for Internet of Things (IoT) devices?

- ☐ Verify access control lists to the database where collected data is stored.
- ☐ Confirm that acceptable limits of data bandwidth are defined for each device.
- ☐ Ensure that message queue telemetry transport (MQTT) is used.
- ☒ Determine how devices are connected to the local network.

Question 372

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

- ☐ In symmetric key encryption the same key is used for encryption and decryption where as asymmetric key uses private key for encryption and decryption
- ☐ In symmetric key encryption the public key is used for encryption and the symmetric key for decryption. Where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption
- ☒ In symmetric key encryption the same key is used for encryption and decryption where as in asymmetric key encryption the public key is used for encryption and private key is used for decryption.
- ☐ Both uses private key for encryption and the decryption process can be done using public key

Explanation:

Explanation:

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

Symmetric Encryption

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

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

Asymmetric Encryption

The problem with secret keys is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. One answer is the usage of asymmetric encryption, in which there are two related keys,

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

usually called a key pair. The public key is made freely available to anyone who might want to send you a message. The second key, called the private key is kept secret, so that only you know it.

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

This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public).A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

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

The following were incorrect answers:

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

Reference:

CISA review manual 2014 Page number 348 and 349

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

Question 373

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

- ☐ Minimizing costs for the services provided
- ☐ Prohibiting the provider from subcontracting services
- ☐ Evaluating the process for transferring knowledge to the IT department
- ☒ Determining if the services were provided as contracted

Explanation:

Explanation:

From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is

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

acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department.

Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

Question 374

The PRIMARY objective of an audit of IT security policies is to ensure that:

- ☐ they are distributed and available to all staff.
- ☒ security and control policies support business and IT objectives.
- ☐ there is a published organizational chart with functional descriptions.
- ☐ duties are appropriately segregated.

Explanation:

Explanation:

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

Question 375

Which of the following provides the BEST indication that the information security program is in alignment with enterprise requirements?

- ☐ The security strategy is benchmarked with similar organizations.
- ☐ The information security manager reports to the chief executive officer.
- ☐ An IT governance committee is in place.
- ☒ Security strategy objectives are defined in business terms.

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

Question 376

Which of the following is the MOST effective mechanism for ensuring that critical IT operational problems are reported to executive management in a timely manner?

- ☐ Regular meetings
- ☐ Escalation procedures
- ☒ Service level monitoring
- ☐ Periodic status reports

Question 377

Which of the following is the MOST important part of an incident response plan?

- ☐ Recovery point objective (RPO)
- ☒ Recovery time objective (RTO)
- ☐ Mean time to report (MTR)
- ☐ Business impact analysis (BIA)

Question 378

An IS auditor is reviewing a bank's service level agreement (SLA) with a third-party provider that hosts the bank's secondary data center. Which of the following findings should be of GREATEST concern to the auditor?

- ☐ The recovery point objective (RPO) has a shorter duration than documented in the disaster recovery plan
- ☒ The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan
- ☐ Backup data is hosted online only
- ☐ The SLA has not been reviewed in more than a year

Question 379

If a database is restored from information backed up before the last system image, which of the following is recommended?

- ☐ The system should be restarted after the last transaction.
- ☒ The system should be restarted before the last transaction.
- ☐ The system should be restarted at the first transaction.
- ☐ The system should be restarted on the last transaction.

Explanation:

Explanation:

If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

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

Question 380

After discussing findings with an auditee, an IS auditor is required to obtain approval of the report from the CEO before issuing it to the audit committee. This requirement PRIMARILY affects the IS auditor's:

- ☐ judgment
- ☐ effectiveness
- ☒ independence
- ☐ integrity

Question 381

Responsibility and reporting lines cannot always be established when auditing automated systems since:

- ☐ diversified control makes ownership irrelevant.
- ☐ staff traditionally changes jobs with greater frequency.
- ☒ ownership is difficult to establish where resources are shared.
- ☐ duties change frequently in the rapid development of technology.

Explanation:

Explanation:

Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

Question 382

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.

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

Question 383

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 384

An IS auditor performs a follow-up audit and learns the approach taken by the auditee to fix the findings differs from the agreed-upon approach confirmed during the last audit. Which of the following should be the auditor's NEXT course of action?

- ☐ Inform senior management of the change in approach.
- ☐ Conduct a risk analysis incorporating the change.
- ☒ Report results of the follow-up to the audit committee.
- ☐ Evaluate the appropriateness of the remedial action taken.

Question 385

Before implementing controls, management should FIRST ensure that the controls:

- ☒ satisfy a requirement in addressing a risk issue.
- ☐ do not reduce productivity.
- ☐ are based on a cost-benefit analysis.
- ☐ are detective or corrective.

Explanation:

Explanation:

When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

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

Question 386

Which of the following is the BEST reason to utilize blockchain technology to record accounting transactions?

- ☒ Integrity of records
- ☐ Confidentiality of records
- ☐ Availability of records
- ☐ Distribution of records

Question 387

Which audit technique provides the GREATEST assurance that incident management procedures are effective?

- ☐ Determining whether incidents are categorized and addressed
- ☒ Performing comprehensive vulnerability scanning and penetration testing
- ☐ Comparing incident management procedures to best practices
- ☐ Evaluating end-user satisfaction survey results

Question 388

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager would be to:

- ☐ review the state of security awareness
- ☐ perform a gap analysis
- ☒ perform a risk assessment
- ☐ review information security policies

Question 389

Which of the following firewall technologies involves examining the header of every packet of data traveling between the Internet and the corporate network without examining the previous packets?

- ☐ Proxy servers
- ☐ Bastion host
- ☐ Stateful filtering
- ☒ Stateless filtering

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

Question 390

The initial step in establishing an information security program is the:

- ☐ development and implementation of an information security standards manual.
- ☐ performance of a comprehensive security control review by the IS auditor.
- ☒ adoption of a corporate information security policy statement.
- ☐ purchase of security access control software.

Explanation:

Explanation:

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

Question 391

An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?

- ☐ Allow changes to be made only with the DBA user account.
- ☐ Make changes to the database after granting access to a normal user account.
- ☒ Use the DBA user account to make changes, log the changes and review the change log the following day.
- ☐ Use the normal user account to make changes, log the changes and review the change log the following day.

Explanation:

Explanation:

The use of a database administrator (DBA) user account is normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. The use of the DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

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

Question 392

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 393

Which of the following is the MAIN advantage of using one-time passwords?

- ☐ They are suitable for e-commerce authentication.
- ☐ Passwords are hardware/software generated.
- ☒ An intercepted password would be of no use.
- ☐ The user does not need to remember passwords.

Question 394

A technical lead who was working on a major project has left the organization. The project manager reports suspicious system activities on one of the servers that is accessible to the whole team. What would be of GREATEST concern if discovered during a forensic investigation?

- ☒ Audit logs are not enabled for the system
- ☐ A logon ID for the technical lead still exists
- ☐ Spyware is installed on the system
- ☐ A Trojan is installed on the system

Explanation:

Explanation:

Audit logs are critical to the investigation of the event; however, if not enabled, misuse of the logon ID of the technical lead and the guest account could not be established. The logon ID of the technical lead should have been deleted as soon as the employee left the organization but, without audit logs, misuse of the ID is difficult to prove. Spyware installed on the system is a concern but could have been installed by any user and, again, without the presence of logs, discovering who installed the spyware is difficult. A Trojan installed on the system is a concern, but it can be done by any user as it is accessible to the whole group and, without the presence of logs, investigation would be difficult.

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

Question 395

A client/server configuration will:

- ☒ optimize system performance by having a server on a front-end and clients on a host
- ☐ enhance system performance through the separation of front-end and back-end processes
- ☐ keep track of all the clients using the IS facilities of a service organization
- ☐ limit the clients and servers' relationship by limiting the IS facilities to a single hardware system

Question 396

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 397

Which of the following is the PRIMARY responsibility of an organization's IT steering committee?

- ☐ Reporting on key performance measures
- ☒ Communicating strategic goals to IT project teams
- ☐ Conducting peer reviews of other organizations
- ☐ Identifying new technological threats

Question 398

An IS auditor is auditing the infrastructure of an organization that hosts critical applications withing a virtual environment. Which of the following is MOST important for the auditor to focus on?

- ☐ The ability to copy and move virtual machines in real time
- ☒ The controls in place to prevent compromise of the host
- ☐ Issues arising from system management of a virtual infrastructure
- ☐ Qualifications of employees managing the applications

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

Question 399

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 400

Which of the following is a prerequisite to help ensure that IS hardware and software support the delivery of mission-critical functions?

- ☐ Control over IS infrastructure expenditure
- ☐ An independent audit of the process
- ☒ A comprehensive IS applications architecture
- ☐ Documented emergency change procedures

Question 401

An organization was recently notified by its regulatory body of significant discrepancies in its reporting data. A preliminary investigation revealed that the discrepancies were caused by problems with the organization's data quality. Management has directed the data quality team to enhance their program. The audit committee has asked internal audit to be advisors to the process. After the data quality team identifies the system data at fault, which of the following should internal audit recommend as the NEXT step in the process?

- ☒ Create business rules that validate data quality.
- ☐ Develop an improvement plan.
- ☐ Identify the root cause of data quality problems.
- ☐ Identify the source data owners.

Question 402

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:

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

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 403

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 404

An organization is currently replacing its accounting system. Which of the following strategies will BEST minimize risk associated with the loss of data integrity from the upgrade?

- ☐ Pilot implementation
- ☒ Functional integration testing
- ☐ Fallback contingency
- ☐ Parallel implementation

Question 405

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

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

are designed to detect and address an attack in progress and stop it as soon as possible. A honeypot allows the attack to continue, so as to obtain information about the hacker's strategy and methods.

Question 406

A major portion of what is required to address nonrepudiation is accomplished through the use of:

- ☐ strong methods for authentication and ensuring data validity
- ☒ strong methods for authentication and ensuring data integrity.
- ☐ strong methods for authorization and ensuring data integrity.
- ☐ strong methods for authentication and ensuring data reliability.
- ☐ None of the choices.

Explanation:

Explanation:

A major portion of what is required to address nonrepudiation is accomplished through the use of strong methods for authentication and ensuring data integrity.

Question 407

When removing a financial application system from production, which of the following is MOST important?

- ☐ Media used by the retired system has been sanitized.
- ☒ Data retained for regulatory purposes can be retrieved.
- ☐ End-user requests for changes are recorded and tracked.
- ☐ Software license agreements are retained.

Question 408

The security level of a private key system depends on the number of:

- ☒ encryption key bits.
- ☐ messages sent.
- ☐ keys.
- ☐ channels used.

Explanation:

Explanation:

The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

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

Question 409

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- ☐ Test data run
- ☐ Code review
- ☒ Automated code comparison
- ☐ Review of code migration procedures

Explanation:

Explanation:

An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

Question 410

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

- ☐ There are a number of external modems connected to the network.
- ☐ Users can install software on their desktops.
- ☐ Network monitoring is very limited.
- ☒ Many user IDs have identical passwords.

Explanation:

Explanation:

Exploitation of a known user ID and password requires minimal technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user IDs have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high {for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

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

Question 411

Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

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

Explanation:

Explanation:

Phishing technique include social engineering, link manipulation or web site forgery techniques.

For your exam you should know the information below:

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

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

Link manipulation

Most methods of phishing use some form of technical deception designed to make a link in an email (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishes. In the following example URL, http://www.yourbank.example.com/, it appears as though the URL will take you to the example section of the your bank website; actually this URL points to the "your bank" (i.e. phishing) section of the example website. Another common trick is to make the displayed text for a link (the text between the tags) suggest a reliable destination, when the link actually goes to the phishes' site. The following example link, //en.wikipedia.org/wiki/Genuine, appears to direct the user to an article 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

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

them. Hovering your cursor over the link for a couple of seconds may do a similar thing, but this can still be set by the phishes through the HTML tooltip tag.

Website forgery

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

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

The following answers are incorrect:

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

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

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

Reference:

CISA review manual 2014 Page number 323

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

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

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

Question 412

Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems:

- ☐ desktop systems
- ☐ laptop systems
- ☐ handheld PDAs
- ☒ business-critical systems
- ☐ None of the choices.

Explanation:

Explanation:

Fault-tolerance enables a system to continue operating properly in the event of the failure of some parts of it. It avoids total breakdown, and is particularly sought-after in high-availability environment full of business critical systems.

Question 413

Senior management has allocated funding to each of the organization's divisions to address information security vulnerabilities. The funding is based on each division's technology budget from the previous fiscal year. Which of the following should be of GREATEST concern to the information security manager?

- ☐ Redundant controls may be implemented across divisions
- ☐ Information security governance could be decentralized by divisions
- ☒ Areas of highest risk may not be adequately prioritized for treatment
- ☐ Return on investment may be inconsistently reported to senior management

Question 414

When creating a new risk management program, it is CRITICAL to consider:

- ☐ the risk appetite.
- ☒ compliance measures.
- ☐ risk mitigation techniques.
- ☐ resource utilization.

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

Question 415

Which of the following type of lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor/reader to gain access?

- ☐ Bolting door locks
- ☐ Combination door lock
- ☒ Electronic door lock
- ☐ Biometric door lock

Explanation:

Explanation:

Electronic door lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

For CISA exam you should know below types of lock

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

Electronic door lock – This system uses a magnetic or embedded chip based plastic card key or token entered into a sensor reader to gain access. A special code internally stored in the card or token is read by sensor device that then activates the door locking mechanism.

The Combination door lock or cipher lock uses a numeric key pad or dial to gain entry, and is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

The following were incorrect answers:

Bolting door lock – These locks required the traditional metal key to gain entry. The key should be stamped “do not duplicate” and should be stored and issued under strict management control.

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

Biometric door lock – An individual's unique body features such as voice, retina, fingerprint, hand geometry or signature, activate these locks. This system is used in instances when extremely sensitive facilities must be protected such as in the military.

The Combination door lock or cipher lock uses a numeric key pad or dial to gain entry, and is often seen at airport gate entry doors and smaller server rooms. The combination should be changed at regular interval or whenever an employee with access is transferred, fired or subject to disciplinary action. This reduces risk of the combination being known by unauthorized people.

Reference:

CISA review manual 2014 Page number 376

Question 416

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- ☐ avoidance
- ☐ transference
- ☒ mitigation
- ☐ acceptance

Explanation:

Explanation:

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

Question 417

A firm is considering using biometric fingerprint identification on all PCs that access critical datA. This requires:

- ☒ that a registration process is executed for all accredited PC users.
- ☐ the full elimination of the risk of a false acceptance.
- ☐ the usage of the fingerprint reader be accessed by a separate password.
- ☐ assurance that it will be impossible to gain unauthorized access to critical data.

Explanation:

Explanation:

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

The fingerprints of accredited users need to be read, identified and recorded, i.e., registered, before a user may operate the system from the screened PCs. Choice B is incorrect, as the false- acceptance risk of a biometric device may be optimized, but will never be zero because this would imply an unacceptably high risk of false rejection. Choice C is incorrect, as the fingerprint device reads the token (the user's fingerprint) and does not need to be protected in itself by a password. Choice Dis incorrect because the usage of biometric protection on PCs does not guarantee that other potential security weaknesses in the system may not be exploited to access protected data.

Question 418

An organization is designing an application programming interface (API) for business-to-business data sharing with a vendor. Which of the following is the BEST way to reduce the potential risk of data leakage?

- ☐ Implement a policy to require data transfer over hypertext transfer protocol (HTTP)
- ☒ Implement the API on a secure server and encrypt traffic between both organizations
- ☐ Restrict the allowable number of API calls within a specified period
- ☐ Conduct an independent review of the application architecture and service level agreements (SLAs)

Question 419

Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:

- ☐ almost always less efficient.
- ☐ almost always less effective.
- ☐ almost always less secure.
- ☐ almost always less costly to setup.
- ☒ None of the choices.

Explanation:

Explanation:

Early attempts at producing firewalls operated at the application level of the seven-layer OSI model but this required too much CPU processing power.

Packet filters operate at the network layer and function more efficiently because they only look at the header part of a packet. NO FIREWALL operates at the physical level.

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

Question 420

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 421

Which of the following will prevent dangling tuples in a database?

- ☐ Cyclic integrity
- ☐ Domain integrity
- ☐ Relational integrity
- ☒ Referential integrity

Explanation:

Explanation:

Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., for existence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized source documentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

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

Question 422

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 423

When following up on a data breach, an IS auditor finds a system administrator may have compromised the chain of custody. Which of the following should the system administrator have done FIRST to preserve the evidence?

- ☐ Perform forensic discovery
- ☐ Notify key stakeholders
- ☒ Quarantine the system
- ☐ Notify the incident response team

Question 424

The role of the certificate authority (CA) as a third party is to:

- ☐ provide secured communication and networking services based on certificates.
- ☐ host a repository of certificates with the corresponding public and secret keys issued by that CA.
- ☐ act as a trusted intermediary between two communication partners.
- ☒ confirm the identity of the entity owning a certificate issued by that CA.

Explanation:

Explanation:

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

The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued. Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would not be archived at the CA. The CA can contribute to authenticating the communicating partners to each other, but the CA is not involved in the communication stream itself.

Question 425

Which of the following application input controls would MOST likely detect data input errors in the customer account number field during the processing of an accounts receivable transaction?

- ☒ Validity check
- ☐ Reasonableness check
- ☐ Parity check
- ☐ Limit check

Question 426

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

- ☐ Halon gas
- ☐ Deluge sprinklers
- ☒ Dry-pipe sprinklers
- ☐ Wet-pipe sprinklers

Explanation:

Explanation:

Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

Question 427

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

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

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 428

When conducting a penetration test of an IT system, an organization should be MOST concerned with:

- ☐ the confidentiality of the report.
- ☐ finding all possible weaknesses on the system.
- ☒ restoring all systems to the original state.
- ☐ logging all changes made to the production system.

Explanation:

Explanation:

All suggested items should be considered by the system owner before agreeing to penetration tests, but the most important task is to be able to restore all systems to their original state.

Information that is created and/or stored on the tested systems should be removed from these systems. If for some reason, at the end of the penetration test, this is not possible, all files (with their location) should be identified in the technical report so that the client's technical staff will be able to remove these after the report has been received.

Question 429

A maturity model can be used to aid the implementation of IT governance by identifying:

- ☐ critical success factors (CSF)
- ☐ performance drivers
- ☒ improvement opportunities
- ☐ accountabilities

Question 430

Which of the following terms refers to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders?

- ☒ ILD&P
- ☐ ICT&P
- ☐ ILP&C
- ☐ ILR&D
- ☐ None of the choices.

Explanation:

Explanation:

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

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 431

How does the SSL network protocol provide confidentiality?

- ☐ Through symmetric encryption such as RSA
- ☐ Through asymmetric encryption such as Data Encryption Standard, or DES
- ☐ Through asymmetric encryption such as Advanced Encryption Standard, or AES
- ☒ Through symmetric encryption such as Data Encryption Standard, or DES

Explanation:

Explanation:

The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption.

Standard, or DES.

Question 432

Which of the following is MOST critical to the successful implementation of information security within an organization?

- ☐ Strong risk management skills exist within the information security group.
- ☐ Budget is allocated for information security tools.
- ☐ The information security manager is responsible for setting information security policy.
- ☒ Security is effectively marketed to all managers and employees.

Question 433

The specific advantage of white box testing is that it:

- ☐ verifies a program can operate successfully with other parts of the system.
- ☐ ensures a program's functional operating effectiveness without regard to the internal program structure.
- ☒ determines procedural accuracy or conditions of a program's specific logic paths.
- ☐ examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Explanation:

Explanation:

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

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

Question 434

Which of the following audit is mainly designed to evaluate the internal control structure in a given process or area?

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

Explanation:

Explanation:

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

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

What is an audit?

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

Compliance Audit

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

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

specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

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

Financial Audit

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

Operational Audit

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

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

Objectives

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

To understand the responsibilities and risks faced by an organization.

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

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

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

Integrated Audits

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

IS Audit

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

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

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

Forensic Audit

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

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

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

The following answers are incorrect:

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

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

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

Reference:

CISA Review Manual 2014 Page number 44

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

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

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

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

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

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

Question 435

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a pattern of behaviors, effects, assumptions, attitude and ways of doing things?

- ☐ Governing
- ☒ Culture
- ☐ Enabling and support
- ☐ Emergence

Explanation:

Explanation:

Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

For your exam you should know the information below.

Business Model for Information Security

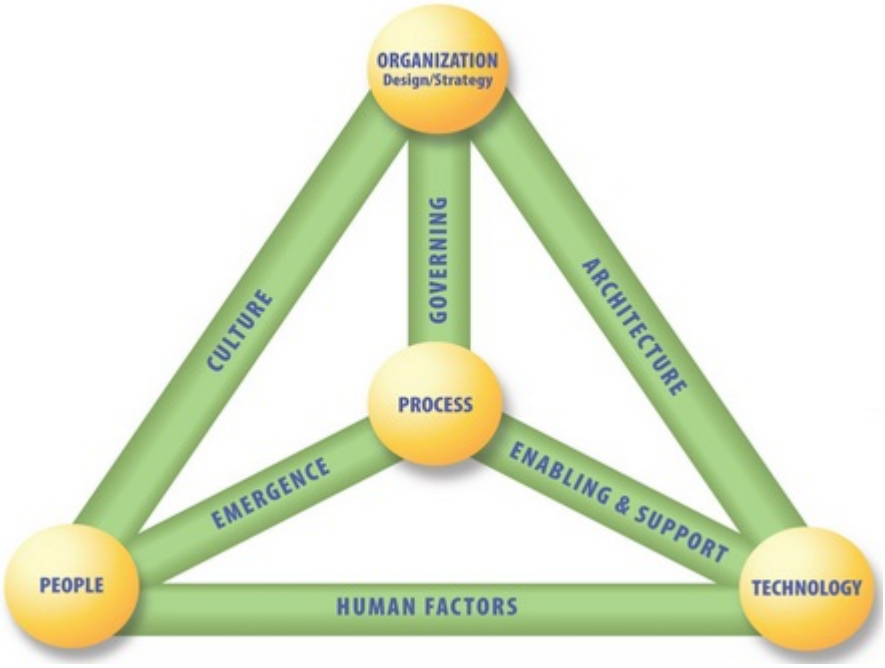
The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The BMIS takes a business-oriented approach to managing information security, building on the foundational concepts developed by the Institute. The model utilizes systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage security. The elements and dynamic interconnections that form the basis of the model establish the boundaries of an information security program and model how the program functions and reacts to internal and external change. The BMIS provides the context for frameworks such as Cubit.

The essence of systems theory is that a system needs to be viewed holistically – not merely as a sum of its parts – to be accurately understood. A holistic approach examines the system as a complete functioning unit. Another tenet of systems theory is that one part of the system enables understanding of other parts of the system. “Systems thinking” is a widely recognized term that refers to the examination of how systems interact, how complex systems work and why “the whole is more than the sum of its parts.” Systems theory is most accurately described as a complex network of events, relationships, reactions, consequences, technologies, processes and people that interact in often unseen and unexpected ways. Studying the behaviors and results of the interactions can assist the manager to better understand the organizational system and the way it functions. While

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

management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.

All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

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.

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

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People – The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:

Recruitment strategies (access, background checks, interviews, roles and responsibilities)

Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)

Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process – Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.

Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology – Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.

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

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

reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing – Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

2. Culture – Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support – The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

4. Emergence – Emergence – which connotes surfacing, developing, growing and evolving – refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

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

5. Human factors – The human factors dynamic interconnection represents the interaction and gap between technology and people and, as such, is critical to an information security program. If people do not understand how to use the technology, do not embrace the technology or will not follow pertinent policies, serious security problems can evolve. Internal threats such as data leakage, data theft and misuse of data can occur within this dynamic interconnection. Human factors may arise because of age, experience level and/or cultural experiences. Because human factors are critical components in maintaining balance within the model, it is important to train all of the enterprise's human resources on pertinent skills.

6. Architecture – A security architecture is a comprehensive and formal encapsulation of the people, processes, policies and technology that comprise an enterprise's security practices. A robust business information architecture is essential to understanding the need for security and designing the security architecture. It is within the architecture dynamic interconnection that the enterprise can ensure defense in depth. The design describes how the security controls are positioned and how they relate to the overall IT architecture. An enterprise security architecture facilitates security capabilities across lines of businesses in a consistent and a cost-effective manner and enables enterprises to be proactive with their security investment decisions.

The following answers are incorrect:

Governing - Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

Enabling and support - The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Emergence – Emergence – which connotes surfacing, developing, growing and evolving – refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

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

Reference:

CISA review manual 2014 page number 37 and 38

http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

Question 436

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 437

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.

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

Question 438

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:

Explanation:

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

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

The security protocols can either be AH or ESP.

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

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:

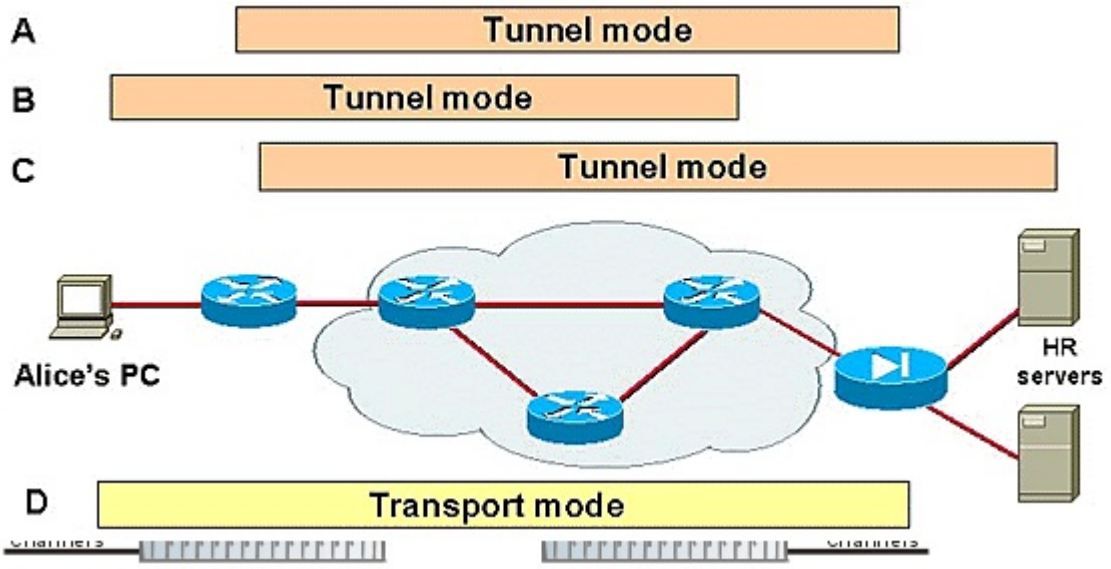
Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.

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.

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

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

FIGURE: 1



IPSEC Transport Mode versus Tunnel Mode

Tunnel and transport modes in IPSec.

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

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

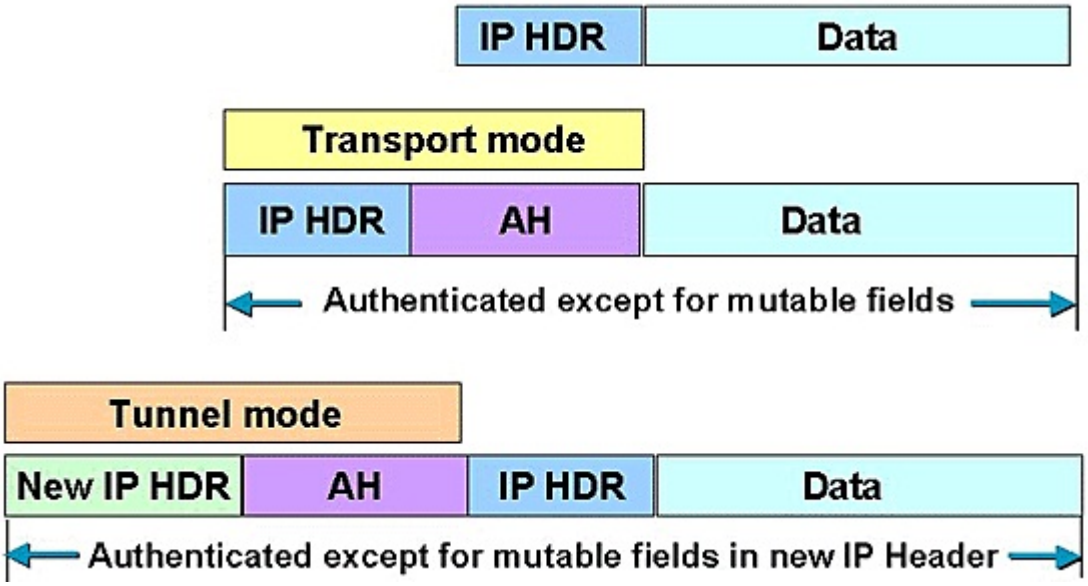
Tunnel mode is also used to connect an end-station running IPSec software, such as the Cisco Secure VPN Client, to an IPSec gateway, as shown in example B.

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.

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

FIGURE: 2



IPSEC AH Tunnel and Transport mode

AH Tunnel Versus Transport Mode

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

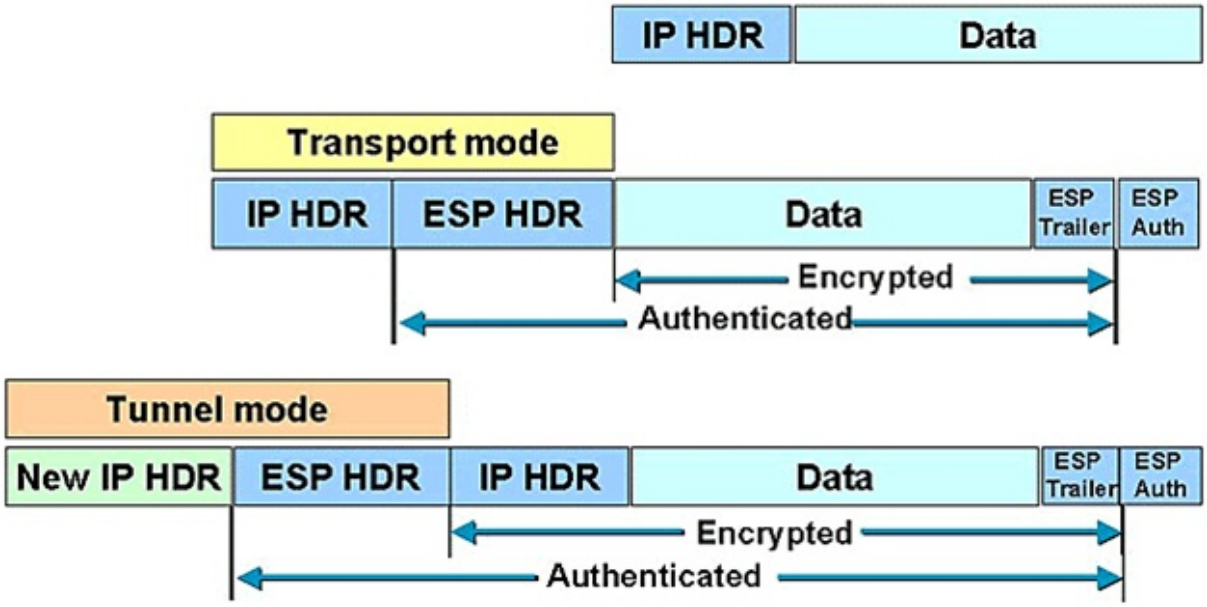
As you can see in Figure 2 above, In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.

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

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



ESP Tunnel Versus Transport Mode

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

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

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

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

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.

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

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:

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

and

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

and

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

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

Question 439

At a hospital, medical personal carry handheld computers which contain patient health data. These handheld computers are synchronized with PCs which transfer data from a hospital database. Which of the following would be of the most importance?

- ☒ The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
- ☐ The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
- ☐ Timely synchronization is ensured by policies and procedures.
- ☐ The usage of the handheld computers is allowed by the hospital policy.

Explanation:

Explanation:

Data confidentiality is a major requirement of privacy regulations. Choices B, C and D relate to internal security requirements, and are secondary when compared to compliance with data privacy laws.

Question 440

Which of the following would a digital signature MOST likely prevent?

- ☒ Corruption
- ☐ Unauthorized change
- ☐ Repudiation
- ☐ Disclosure

Explanation:

Explanation:

The main reason of using digital signature is to ensure message integrity.it also helps to ensure authenticity and non-repudiation of the message. A digital signature can never ensure the confidentiality of data

Question 441

An advantage of using sanitized live transactions in test data is that:

- ☐ all transaction types will be included.
- ☐ every error condition is likely to be tested.
- ☐ no special routines are required to assess the results.
- ☒ test transactions are representative of live processing.

Explanation:

Explanation:

Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

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

Question 442

Which of the following would MOST effectively reduce social engineering incidents?

- ☒ Security awareness training
- ☐ increased physical security measures
- ☐ E-mail monitoring policy
- ☐ intrusion detection systems

Explanation:

Explanation:

Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e- mail in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

Question 443

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

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

Explanation:

Explanation:

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

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

Question 444

Which of the following is BEST enabled by following a configuration management process for new applications?

- ☐ Deploying approved emergency changes to production
- ☐ Ensuring proper testing of code before deployment
- ☐ Managing successful implementation of acquired software
- ☒ Maintaining adequate control over changes to production

Question 445

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:

Explanation:

The LEAST is the keyword used in this question, You need to find out a LEAST important factor in the measurement of the productivity.

For the CISA exam you should know the table below which contains information about measurement of a critical success factor.

Measurement of Critical Success Factors

Productivity

Dollars spent per use

Number of transactions per month

Number of transactions per user

Quality

Number of discrepancies

Number of disputes

Number of occurrences of fraud/misuse detection

Economic value

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

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.

Reference:

CISA review manual 2014 Page number 159

Question 446

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 447

The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

- ☒ only the sender and receiver are able to encrypt/decrypt the data.
- ☐ the sender and receiver can authenticate their respective identities.
- ☐ the alteration of transmitted data can be detected.
- ☐ the ability to identify the sender by generating a one-time session key.

Explanation:

Explanation:

SSL generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality. Although SSL allows the exchange of X509 certificates to provide for identification and authentication, this feature along with choices C and D are not the primary objectives.

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

Question 448

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 449

Which of the following should be the MOST important consideration when determining which information system application to audit?

- ☐ Cost-benefit analysis
- ☐ Available resources
- ☒ Business impact analysis
- ☐ Newly implemented systems

Question 450

Which of the following should be the PRIMARY concern of an IS auditor during a review of an external IT service level agreement (SLA) for computer operations?

- ☐ No employee succession plan
- ☒ Changes in services are not tracked
- ☐ Lack of software escrow provisions
- ☐ Vendor has exclusive control of IT resources

Question 451

Digital signatures require the:

- ☐ signer to have a public key and the receiver to have a private key.
- ☒ signer to have a private key and the receiver to have a public key.
- ☐ signer and receiver to have a public key.
- ☐ signer and receiver to have a private key.

Explanation:

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

Explanation:

Digital signatures are intended to verify to a recipient the integrity of the data and the identity of the sender. The digital signature standard is a public key algorithm. This requires the signer to have a private key and the receiver to have a public key.

Question 452

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 453

When an information security manager presents an information security program status report to senior management, the MAIN focus should be:

- ☒ key performance indicators (KPIs)
- ☐ critical risks indicators
- ☐ net present value (NPV)
- ☐ key controls evaluation

Question 454

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.

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

Question 455

Which of the following would be MOST important for an IS auditor to review during an audit of an automated continuous monitoring process being used by the finance department?

- ☐ Resiliency of the monitoring service
- ☒ Dual control and approvals embedded in processes
- ☐ Management sign-off of test documentation
- ☐ Configuration of the monitoring tool

Question 456

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 457

An objective of capacity management is to ensure that:

- ☒ organizational resources are used efficiently.
- ☐ available resources are fully utilized.
- ☐ new resources are allocated for new applications.
- ☐ resource utilization does not drop below 85%.

Question 458

A purpose of project closure is to determine the:

- ☐ potential risks affecting the quality of deliverables.
- ☒ lessons learned for use in future projects.
- ☐ project feasibility requirements
- ☐ professional expertise of the project manager.

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

Question 459

A database audit reveals an issue with the way data ownership for client data is defined. Which of the following roles should be accountable for this finding?

- ☐ Business management
- ☒ Database administrator
- ☐ Information security management
- ☐ Privacy manager

Question 460

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 461

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.

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

Question 462

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 463

Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?

- ☐ datagram scanning
- ☒ access lists
- ☐ stateful inspection
- ☐ state checking
- ☐ link progressing
- ☐ None of the choices.

Explanation:

Explanation:

In addition to deploying stateful firewall, you may setup basic traffic filtering on a more sophisticated router. As an example, on a Cisco IOS based router you may use ip access lists (ACL) to perform basic filtering on the network edge. Note that if they have denied too much traffic, something is obviously being too restrictive and you may want to reconfigure them.

Question 464

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

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

Explanation:

Explanation:

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

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

Question 465

Which of the following BEST describes an audit risk?

- ☒ The financial report may contain undetected material errors.
- ☐ The company is being sued for false accusations.
- ☐ Key employees have not taken vacation for 2 years.
- ☐ Employees have been misappropriating funds.

Question 466

Statistical sampling is NOT based on which of the following audit sample techniques?

- ☒ Haphazard Sampling
- ☐ Random Sampling
- ☐ Cell Sampling
- ☐ Fixed interval sampling

Explanation:

Explanation:

The NOT keyword is used in the question. You need find out an option which is NOT an example of statistical sampling. Statistical sampling is NOT based on Haphazard sampling.

For your exam you should know the information below

Audit samples are selected for the purpose of collecting representative evidence to be subjected to either compliance testing or substantive testing. The auditor should consider a selection technique that will provide the most relevant evidence supported by appropriate analytical procedures.

Two basic types of audit samples can be designed by the auditor to fulfill their requirements:

statistical and no statistical. Below Figure shows the various audit samples, as well as their testing methods. Care is given to the selection process in order to avoid drawing the wrong conclusion from the wrong sample. This is referred to as a sampling risk. Let's look at each of these samples more closely.

Statistical Sampling

Statistical sampling uses mathematical techniques that result in an outcome that is mathematically quantifiable. Statistical samples are usually presented as a percentage. The purpose of statistical sampling is to gain an objective representation. Samples are selected by an objective mathematical process. The auditor should be aware that if the client has strong internal controls, the sample sizes may be smaller because the odds of fraud or failure will be lower.

Examples of statistical sampling include the following:

Random sampling Samples are selected at random.

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

Cell sampling Random selection is performed at predefined intervals.

Fixed interval sampling The sample existing at every n + interval increment is selected for testing.

No statistical Sampling

No statistical sampling is based on the auditor's judgment (also referred to as judgmental sampling). The auditor determines the sample size, the method of generating the sample, and the number of items to be analyzed. The results of judgmental sampling are unlikely to represent the actual population. This is a subjective process usually based on elements of risk or materiality. An example of no statistical sampling includes haphazard sampling, in which the samples are randomly drawn for testing.

After the samples are selected, the next step is to perform compliance tests or substantive testing.

Conducting Audit Testing As stated earlier, the basic test methods used will be either compliance testing or substantive testing. Appropriate audit samples will have to be generated for the test.

Compliance Testing

Compliance testing tests for the presence or absence of something. Compliance testing includes verifying that policies and procedures have been put in place, and checking that user access rights, program change control procedures, and system audit logs have been activated. An example of a compliance test is comparing the list of persons with physical access to the data center against the HR list of current employees.

Compliance testing is based on one of the following types of audit samples:

Attribute sampling Generally popular in compliance testing. The objective is to determine whether an attribute is present or absent in the subject sample. The result is specified by the rate of occurrence—for example, the presence of 1 in 100 units would be 1 percent.

Stop-and-go sampling Used when few errors are expected. Stop-and-go allows the test to occur without excessive effort in sampling and provides the opportunity to stop testing at the earliest possible opportunity. It is a simple form of testing to reinforce any claim that errors are unlikely in the sample population.

Discovery sampling A 100 percent sampling used to detect fraud or when the likelihood of evidence existing is low. Forensics is an excellent example of discovery sampling. This is an attempt to discover evidence.

Precision, or expected error rate The precision rate indicates the acceptable margin of error between audit samples and the total quantity of the subject population. This is usually expressed as a percentage, such as 5 percent. To obtain a very low error rate, it is necessary to use a very large sample in testing. Auditors are justified in using a smaller sample size when the total population is expected to be error-free. A larger sample is required when errors are expected to be present in the

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

population. The larger sample can yield a higher average. When errors are expected, the auditor must examine more data to determine whether the actual errors are within a tolerable error rate (maximum errors you would accept).

Error levels may be determined by reviewing the findings of a prior audit and by considering changes in the organization's procedures. Use the risk-based audit strategy to determine whether your samples and tests are telling the truth about the audited.

Substantive Testing

Substantive testing seeks to verify the content and integrity of evidence. Substantive tests may include complex calculations to verify account balances, perform physical inventory counts, or execute sample transactions to verify the accuracy of supporting documentation. Substantive tests use audit samples selected by dollar value or to project (forecast or estimate) a total for groups with related characteristics.

Substantive testing is based on one of the following types of audit samples:

Variable sampling Used to designate dollar values or weights (effectiveness) of an entire subject population by prorating from a smaller sample. Consider the challenge of counting large volumes of currency by its weight. Variable sampling could be used to count currency by multiplying the physical weight of one unit by the total weight of the combined sample, and then multiplying by the face value printed on the bill or coin. A demonstration is a single $50 bill weighing 1.0 gram, with the entire sample of $50 bills weighing 61 grams altogether. The combined sample weight would indicate a total quantity of 61 bills for an estimated dollar value of $3,050. This is a common technique for forecasting quantity and value of inventory based on particular characteristics.

Unsatisfied mean estimation Used in an attempt to project an estimated total for the whole subject population.

Stratified mean estimation Used to calculate an average by group, similar to demographics, whereby the entire population is divided (stratified) into smaller groups based on similar characteristics.

Examples are teenagers from the ages of 13 to 19, people from the ages of 20 to 29, people from the ages of 30 to 39, and those who are male or female, smokers or nonsmokers, and so on. Difference estimation Used to determine the difference between audited and unaudited claims of value.

The following answers are incorrect:

The other options like Random Sampling, Cell Sampling and Fixed Interval Sampling are examples of Statistical sampling.

Reference:

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

CISA review manual 2014 page number 55 to 56

CISA certified information system auditor study guide Second Edition Page Number 98 to 101

Question 467

The use of a GANTT chart can:

- ☒ aid in scheduling project tasks.
- ☐ determine project checkpoints.
- ☐ ensure documentation standards.
- ☐ direct the post-implementation review.

Explanation:

Explanation:

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

Question 468

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

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

Question 469

When reviewing an organization's data protection practices, an IS auditor should be MOST concerned with a lack of:

- ☐ a security team.
- ☒ data classification.
- ☐ training manuals.
- ☐ data encryption.

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

Question 470

When recommending a preventive control against cross-site scripting in web applications, an information security manager is MOST likely to suggest:

- ☐ using https in place of http.
- ☐ hardening of the web server's operating system.
- ☐ consolidating multiple sites into a single portal.
- ☒ coding standards and code review.

Question 471

Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

- ☒ End-user involvement
- ☐ Senior management involvement
- ☐ Security administration involvement
- ☐ IS auditing involvement

Explanation:

Explanation:

End-user involvement is critical during the business impact assessment phase of business continuity planning.

Question 472

An IS auditor is performing a follow-up audit and notes that some critical deficiencies have not been addressed. The auditor's BEST course of action is to:

- ☒ assess the impact of not addressing deficiencies.
- ☐ document management's reasons for not addressing deficiencies.
- ☐ postpone the audit until the deficiencies are addressed.
- ☐ provide new recommendations.

Question 473

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

- ☒ The preservation of the chain of custody for electronic evidence
- ☐ Time and cost savings
- ☐ Efficiency and effectiveness
- ☐ Ability to search for violations of intellectual property rights

Explanation:

Explanation:

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

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

Question 474

An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

- ☒ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Explanation:

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

Question 475

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

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

Question 476

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.

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

Question 477

An IS auditor concludes that an organization has a quality security policy. Which of the following is MOST important to determine next? The policy must be:

- ☐ updated frequently.
- ☐ developed by process owners.
- ☐ based on industry standards.
- ☒ well understood by all employees.

Question 478

Which of the following statement INCORRECTLY describes network device such as a Router?

- ☐ Router creates a new header for each packet
- ☒ Router builds a routing table based on MAC address
- ☐ Router does not forward broadcast packet
- ☐ Router assigns a different network address per port

Explanation:

Explanation:

The INCORRECTLY keyword is used in the question. You need to find out a statement which is not valid about router. Router builds a routing table based on IP address and not on MAC address.

Difference between Router and Bridge:

Router

Bridge

Creates a new header for each packet

Does not alter header. Only reads the header

Builds routing table based on IP address

Build forwarding table based on MAC address

Assigns a different network address per port

Use the same network address for all ports

Filters traffic based on IP address

Filter traffic based on MAC address

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

Does not forward broadcast packet

Forward broadcast packet

Does not forward traffic that contain destination address unknown to the router

Forward traffic if destination address is unknown to bridge

For your exam you should know below information about network devices:

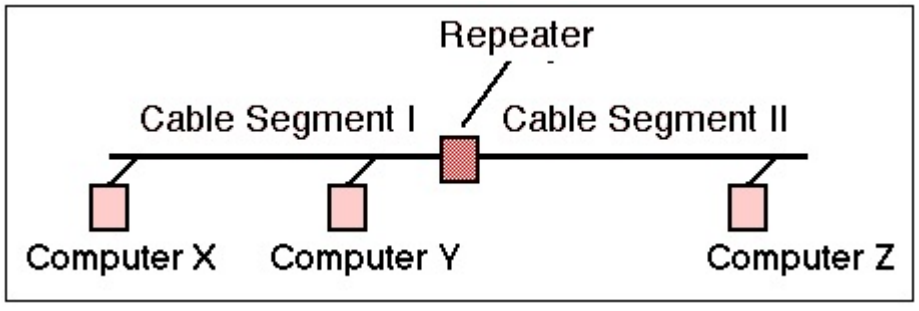
Repeaters

A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.

A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

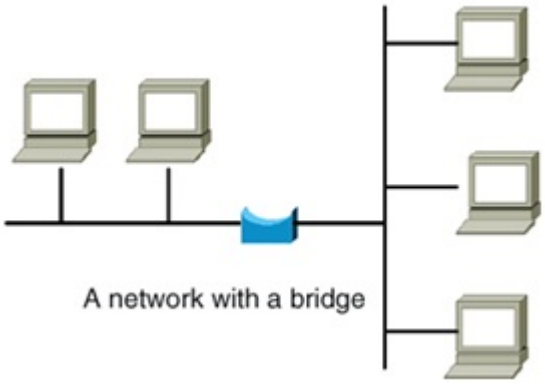


Licensed to Berend Post berend.post@it-university.nl

Bridges

A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge



Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

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

Switches

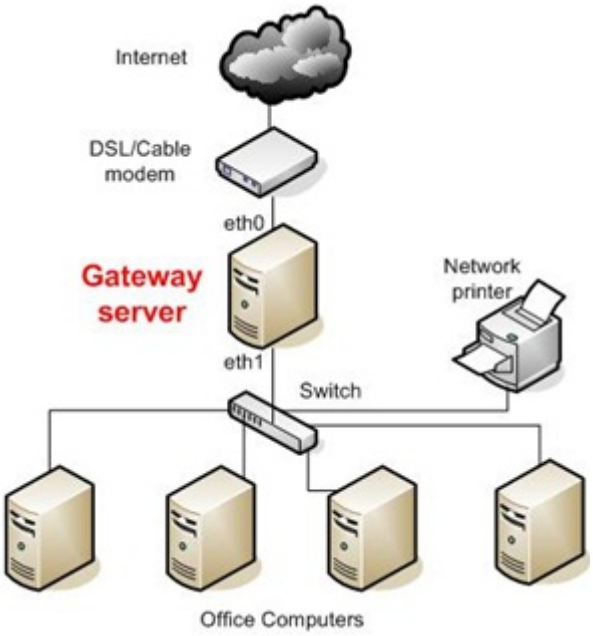
Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions.

Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server



The following were incorrect answers:

The other options presented correctly describes about Router.

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

Reference:

CISA review manual 2014 Page number 263

Question 479

Which of the following should be of GREATEST concern to an IS auditor conducting an audit of an organization's backup processes?

- ☐ A written backup policy is not available.
- ☐ Backup failures are not resolved in a timely manner.
- ☐ The restoration process is slow due to connectivity issues.
- ☒ The service levels are not achieved.

Question 480

Which of the following activities should an IS auditor perform FIRST during an external network security assessment?

- ☐ Exploitation
- ☒ Enumeration
- ☐ Vulnerability scanning
- ☐ Reconnaissance

Question 481

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 482

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

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

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 483

An organization plans to allow third parties to collect customer personal data from a retail loyalty platform via an application programming interface (API). Which of the following should be the PRIMARY consideration when designing this API?

- ☐ Data governance policies
- ☐ System resilience
- ☒ Regulatory compliance
- ☐ Data availability

Question 484

Which of the following is the BEST preventative control to protect the confidentiality of data on a corporate smartphone in the event it is lost?

- ☐ Encryption of the data stored on the device
- ☐ Biometric authentication for the device
- ☐ Password for device authentication
- ☒ Remote data wipe program

Question 485

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:

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:

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

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

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

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

using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

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.

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

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data access layer – his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Reference:

CISA review manual 2014 Page number 188

Question 486

Which of the following should be reviewed as part of a data integrity test?

- ☒ Completeness
- ☐ Confidentiality
- ☐ Data backup
- ☐ Redundancy

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

Question 487

A hub is a device that connects:

- ☐ two LANs using different protocols.
- ☐ a LAN with a WAN.
- ☐ a LAN with a metropolitan area network (MAN).
- ☒ two segments of a single LAN.

Explanation:

Explanation:

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device.

Question 488

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 489

In an environment where most IT services have been outsourced, continuity planning is BEST controlled by:

- ☐ outsourced service provider management.
- ☐ business management.
- ☒ continuity planning specialists.
- ☐ IT management.

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

Question 490

As part of an audit response, an auditee has concerns with the recommendations and is hesitant to implement them. Which of the following would be the BEST course of action for the IS auditor?

- ☐ Accept the auditee's response and perform additional testing.
- ☒ Conduct further discussions with the auditee to develop a mitigation plan.
- ☐ Suggest hiring a third-party consultant to perform a current state assessment.
- ☐ Issue a final report without including the opinion of the auditee.

Question 491

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 492

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 493

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 494

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:

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

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.

Reference:

CISA review manual 2014 Page number 332

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

Question 495

A company is using a software developer for a project. At which of the following points should the software quality assurance (QA) plan be developed?

- ☐ As part of software definition
- ☐ During the feasibility phase
- ☐ Prior to acceptance testing
- ☒ As part of the design phase

Question 496

Which of the following will BEST protect the confidentiality of data stored on the hard drive of a laptop computer?

- ☒ Encryption of the data
- ☐ A boot password
- ☐ Physical locks and alarms
- ☐ Biometric access control

Question 497

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 498

What is the BEST indicator of successful implementation of an organization's information security policy?

- ☐ Reduced number of successful phishing incidents
- ☐ Reduced number of help desk calls
- ☒ Reduced number of noncompliance penalties incurred
- ☐ Reduced number of false-positive security events

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

Question 499

Which of the following is MOST important to the effective management of an end user-developed application?

- ☐ Implementing best practice folder structures
- ☒ Continuous monitoring to facilitate prompt escalation of issues
- ☐ Assigning risk ratings based on probability and impact
- ☐ Stress testing the application through use of data outliers

Question 500

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- ☒ there is an integration of IS and business staffs within projects.
- ☐ there is a clear definition of the IS mission and vision.
- ☐ a strategic information technology planning methodology is in place.
- ☐ the plan correlates business objectives to IS goals and objectives.

Explanation:

Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

Question 501

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

- ☒ Failing to perform user acceptance testing
- ☐ Lack of user training for the new system
- ☐ Lack of software documentation and run manuals
- ☐ Insufficient unit, module, and systems testing

Explanation:

Explanation:

Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

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

Question 502

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:

Explanation:

Blind Testing refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target. Such a testing is expensive, since the penetration tester has to research the target and profile it based on publicly available information.

For your exam you should know below mentioned penetration types

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system is usually the Internet

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such a testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Double Blind Testing -It is an extension of blind testing, since the administrator and security staff at the target are also not aware of test. Such a testing can effectively evaluate the incident handling and response capability of the target.

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:

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

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system 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.

Reference:

CISA review manual 2014 Page number 369

Question 503

Which of the following would provide the MOST important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program?

- ☐ Policies including BYOD acceptable use statements
- ☒ Results of a risk assessment
- ☐ An inventory of personal devices to be connected to the corporate network
- ☐ Findings from prior audits

Question 504

Which of the following is the BEST way for an information security manager to justify continued investment in the information security program when the organization is facing significant budget cuts?

- ☐ Demonstrate an increase in ransomware attacks targeting peer organizations.
- ☐ Demonstrate the readiness of business continuity plans.
- ☐ Demonstrate that implemented program controls are effective.
- ☒ Demonstrate that the program enables business activities.

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

Question 505

During an audit, the client learns that the IS auditor has recently completed a similar security review at a competitor. The client inquires about the competitor's audit results. What is the BEST way for the auditor to address this inquiry?

- ☒ Explain that it would be inappropriate to discuss the results of another audit client.
- ☐ Escalate the question to the audit manager for further action.
- ☐ Discuss the results of the audit omitting specifics related to names and products.
- ☐ Obtain permission from the competitor to use the audit results as examples for future clients.

Question 506

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 507

Which of the following would provide the BEST evidence for an IS auditor to determine whether segregation of duties is in place?

- ☐ A review of the organizational chart
- ☐ A review of personnel files
- ☒ An analysis of user access requests
- ☐ A walk-through of job functions

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

Question 508

Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

- ☐ Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
- ☐ Secure Sockets Layer (SSL) mode
- ☒ Tunnel mode with AH plus ESP
- ☐ Triple-DES encryption mode

Explanation:

Explanation:Tunnel mode provides protection to the entire IP package. To accomplish this, AH and ESP services can be nested. The transport mode provides primary protection for the higher layers of the protocols by extending protection to the data fields (payload) of an IP package. The SSL mode provides security to the higher communication layers (transport layer). The triple-DES encryption mode is an algorithm that provides confidentiality.

Question 509

What is the primary objective of a control self-assessment (CSA) program?

- ☒ Enhancement of the audit responsibility
- ☐ Elimination of the audit responsibility
- ☐ Replacement of the audit responsibility
- ☐ Integrity of the audit responsibility

Explanation:

Explanation:

Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

Question 510

When developing a risk management program, what is the FIRST activity to be performed?

- ☐ Threat assessment
- ☐ Classification of data
- ☒ Inventory of assets
- ☐ Criticality analysis

Explanation:

Explanation:

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

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

Question 511

Which of the following is the BEST method for uncovering shadow IT within an organization?

- ☐ Analyze help desk tickets.
- ☐ Review secondary approval thresholds.
- ☒ Use a cloud access security broker (CASB).
- ☐ Review business processes.

Question 512

Which of the following is MOST important for an information security manager to ensure is included in a business case for a new system?

- ☒ Intangible benefits of the system
- ☐ Risk associated with the system
- ☐ Effectiveness of controls
- ☐ Audit-logging capabilities

Question 513

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

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

Explanation:

Explanation:

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

Question 514

When segregation of duties concerns exists between IT support staff and end users, what would be suitable compensating control?

- ☐ Restricting physical access to computing equipment
- ☒ Reviewing transaction and application logs
- ☐ Performing background checks prior to hiring IT staff
- ☐ Locking user sessions after a specified period of inactivity

Explanation:

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

Explanation:

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

Question 515

An organization's information security department is creating procedures for handling digital evidence that may be used in court. Which of the following would be the MOST important consideration from a risk standpoint?

- ☐ Ensuring the entire security team reviews the evidence
- ☐ Ensuring that analysis is conducted on the original data
- ☐ Ensuring the original data is kept confidential
- ☒ Ensuring the integrity of the data is preserved

Question 516

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 517

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

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

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 518

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

- ☐ Full operational test
- ☒ Preparedness test
- ☐ Paper test
- ☐ Regression test

Explanation:

Explanation:

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery. A paper test is a structured walk- through of the disaster recovery plan and should be conducted before a preparedness test. A full operational test is conducted after the paper and preparedness test. A regression test is not a disaster recovery planning (DRP) test and is used in software maintenance.

Question 519

Which of the following is an attribute of the control self-assessment (CSA) approach?

- ☒ Broad stakeholder involvement
- ☐ Auditors are the primary control analysts
- ☐ Limited employee participation
- ☐ Policy driven

Explanation:

Explanation:

The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, at! of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

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

Question 520

When choosing the best controls to mitigate risk to acceptable levels, the information security manager's decision should be MAINLY driven by:

- ☐ cost-benefit analysis
- ☒ regulatory requirements
- ☐ best practices
- ☐ control framework

Question 521

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

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

Question 522

Which of the following is the BEST way to achieve high availability and fault tolerance for an e-business system?

- ☐ Network diversity
- ☐ Storage area network
- ☒ Robust systems architecture
- ☐ Secure offsite backup storage

Question 523

During development of an information security policy, which of the following would BEST ensure alignment to business objectives?

- ☐ Incorporation of industry best practices
- ☐ Linkage between policy and procedures
- ☒ Use of a balanced scorecard
- ☐ Input from relevant stakeholders

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

Question 524

Which of the following BEST supports an organization's planning efforts for investments in IT initiatives?

- ☐ Capability maturity model
- ☒ Enterprise architecture
- ☐ Agile project management
- ☐ Continuous gap assessment

Question 525

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 526

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.

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

Question 527

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- ☐ The data should be deleted and overwritten with binary 0s.
- ☒ The data should be demagnetized.
- ☐ The data should be low-level formatted.
- ☐ The data should be deleted.

Explanation:

Explanation:

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

Question 528

An organization has suffered a number of incidents in which USB flash drives with sensitive data have been lost. Which of the following would be MOST effective in preventing loss of sensitive data?

- ☐ Modifying the disciplinary policy to be more stringent
- ☐ Implementing a check-in/check-out process for USB flash drives
- ☒ Issuing encrypted USB flash drives to staff
- ☐ Increasing the frequency of security awareness training

Question 529

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

- ☐ users may prefer to use contrived data for testing.
- ☒ unauthorized access to sensitive data may result.
- ☐ error handling and credibility checks may not be fully proven.
- ☐ the full functionality of the new process may not necessarily be tested.

Explanation:

Explanation:

Unless the data are sanitized, there is a risk of disclosing sensitive data.

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

Question 530

During an audit of information security procedures of a large retailer's online store, an IS auditor notes that operating system (OS) patches are automatically deployed upon release. Which of the following should be of GREATEST concern to the auditor?

- ☐ Patches are in conflict with current licensing agreements.
- ☐ Patches are pushed from the vendor increasing Internet traffic.
- ☐ Patches are not reflected in the configuration management database.
- ☒ Patches are not tested before installation on critical servers.

Question 531

What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality?

- ☒ Rapid application development (RAD)
- ☐ GANTT
- ☐ PERT
- ☐ Decision trees

Explanation:

Explanation:

Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

Question 532

Utilizing external resources for highly technical information security tasks allows an information security manager to:

- ☒ transfer business risk.
- ☐ distribute technology risk.
- ☐ outsource responsibility.
- ☐ leverage limited resources.

Question 533

Who should be responsible for network security operations?

- ☐ Business unit managers
- ☒ Security administrators
- ☐ Network administrators
- ☐ IS auditors

Explanation:

Explanation:

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

Security administrators are usually responsible for network security operations.

Question 534

A sales representative is reviewing the organization's feedback blog and gets redirected to a site that sells illegal prescription drugs. The blog site is MOST likely susceptible to which of the following types of attacks?

- ☐ Directory harvesting
- ☐ SQL injection
- ☒ Cross-site scripting
- ☐ Phishing attack.

Question 535

A new regulation requires organizations to report significant security incidents to the regulator within 24 hours of identification. Which of the following is the IS auditor's BEST recommendation to facilitate compliance with the regulation?

- ☒ Include the requirement in the incident management response plan.
- ☐ Establish key performance indicators (KPIs) for timely identification of security incidents.
- ☐ Enhance the alert functionality of the intrusion detection system (IDS).
- ☐ Engage an external security incident response expert for incident handling.

Question 536

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- ☐ Repeatable but Intuitive
- ☒ Defined
- ☐ Managed and Measurable
- ☐ Optimized

Explanation:

Explanation:

Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

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

Question 537

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 538

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 539

What kind of testing should programmers perform following any changes to an application or system?

- ☒ Unit, module, and full regression testing
- ☐ Module testing
- ☐ Unit testing
- ☐ Regression testing

Explanation:

Explanation:

Programmers should perform unit, module, and full regression testing following any changes to an application or system.

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

Question 540

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 541

To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

- ☒ during data preparation.
- ☐ in transit to the computer.
- ☐ between related computer runs.
- ☐ during the return of the data to the user department.

Explanation:

Explanation:

During data preparation is the best answer, because it establishes control at the earliest point.

Question 542

Which of the following is the BEST way to ensure enterprise architectural objectives are aligned with business and technology objectives?

- ☐ Identify dependencies between current and future state technologies.
- ☐ Optimize technology investments with business requirements.
- ☐ Adopt industry-approved architecture standards and best practices.
- ☒ Identify business stakeholder responsibilities for IT projects.

Question 543

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:

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

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 544

An organization has outsourced the development of a core application. However, the organization plans to bring the support and future maintenance of the application back in-house. Which of the following findings should be the IS auditor's GREATEST concern?

- ☐ A training plan for business users has not been developed.
- ☐ The cost of outsourcing is lower than in-house development.
- ☐ The vendor development team is located overseas.
- ☒ The data model is not dearly documented.

Question 545

Which of the following is the MOST important element when developing an information security strategy?

- ☐ Identifying applicable laws and regulations
- ☐ Identifying information assets
- ☐ Determining the risk management methodology
- ☒ Aligning security activities with organizational goals

Question 546

A reduction in which of the following would indicate improved performance in the administration of information security?

- ☐ IT security awareness training days
- ☐ Number of staff involved in security administration
- ☒ Systems subject to an intrusion detection process
- ☐ Turnaround time for requests for new user access

Question 547

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:

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

Explanation:

Security Association (SA)s defines which security parameters should be applied between communication parties as encryption algorithms, key initialization vector, life span of keys, etc.

For your exam you should know the information below about the IPSec protocol:

The IP network layer packet security protocol establishes VPNs via transport and tunnel mode encryption methods.

For the transport method, the data portion of each packet is encrypted, encryption within IPSEC is referred to as the encapsulation security payload (ESP), it is ESP that provides confidentiality over the process.

In the tunnel mode, the ESP payload and its header's are encrypted. To achieve non-repudiation, an additional authentication header (AH) is applied.

In establishing IPSec sessions in either mode, Security Associations (SAs) are established. SAs defines which security parameters should be applied between communicating parties as encryption algorithms, key initialization vector, life span of keys, etc. Within either ESP or AH header, respectively. An SAs is established when a 32-bit security parameter index (SPI) field is defined within the sending host. The SPI is unique identifier that enables the sending host to reference the security parameter to apply, as specified, on the receiving host.

IPSec can be made more secure by using asymmetric encryption through the use of Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows automated key management, use of public keys, negotiation, establishment, modification and deletion of SAs and 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.

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

Authentication Header(AH) – Authentication Header allows authentication of a sender of a data.

Reference:

CISA review manual 2014 Page number 353

Question 548

Who is ultimately responsible and accountable for reviewing user access to systems?

- ☐ Systems security administrators
- ☐ Data custodians
- ☒ Data owners
- ☐ Information systems auditors

Explanation:

Explanation:

Data owners are ultimately responsible and accountable for reviewing user access to systems.

Question 549

During an audit of an enterprise that is dedicated to e-commerce, the IS manager states that digital signatures are used when receiving communications from customers. To substantiate this, an IS auditor must prove that which of the following is used?

- ☐ A biometric, digitalized and encrypted parameter with the customer's public key
- ☒ A hash of the data that is transmitted and encrypted with the customer's private key
- ☐ A hash of the data that is transmitted and encrypted with the customer's public key
- ☐ The customer's scanned signature encrypted with the customer's public key

Explanation:

Explanation:The calculation of a hash, or digest, of the data that are transmitted and its encryption require the public key of the client (receiver) and is called a signature of the message, or digital signature.

The receiver performs the same process and then compares the received hash, once it has been decrypted with their private key, to the hash that is calculated with the received data. If they are the same, the conclusion would be that there is integrity in the data that have arrived and the origin is authenticated. The concept of encrypting the hash with the private key of the originator provides non repudiation, as it can only be decrypted with their public key and, as the CD suggests, the private key would not be known to the recipient. Simply put, in a key-pair situation, anything that can be decrypted by a sender's public key must have been encrypted with their private key, so they must have been the sender, i.e., non-repudiation. Choice C is incorrect because, if this were the case, the

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

hash could not be decrypted by the recipient, so the benefit of non-repudiation would be lost and there could be no verification that the message had not been intercepted and amended. A digital signature is created by encrypting with a private key. A person creating the signature uses their own private key, otherwise everyone would be able to create a signature with any public key. Therefore, the signature of the client is created with the client's private key, and this can be verified—by the enterprise—using the client's public key. Choice B is the correct answer because, in this case, the customer uses their private key to sign the hash data.

Question 550

When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?

- ☐ Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
- ☒ All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
- ☐ Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
- ☐ The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Explanation:

Explanation:

Deleting and formatting does not completely erase the data but only marks the sectors that contained files as being free. There are tools available over the Internet which allow one to reconstruct most of a hard disk's contents. Overwriting a hard disk at the sector level would completely erase data, directories, indices and master file tables. Reformatting is not necessary since all contents are destroyed. Overwriting several times makes useless some forensic measures which are able to reconstruct former contents of newly overwritten sectors by analyzing special magnetic features of the platter's surface. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted. Reconstructing data would be extremely expensive since all analysis must be performed under a clean room atmosphere and is only possible within a short time frame or until the surface is corroded. Data reconstruction from shredded hard disks is virtually impossible, especially when the scrap is mixed with other metal parts. If the transport can be secured and the destruction be proved as described in the option, this is a valid method of disposal.

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

Question 551

An IS auditor discovers that management has created a system interface to receive financial data and store it in a data warehouse. Which of the following provides the BEST assurance that data in the data warehouse is accurate?

- ☐ Established risk management processes
- ☐ A documented change management process
- ☐ Management access reviews
- ☒ Management reconciliations

Question 552

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 553

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 554

Which of the following is the BEST way to control scope creep during application system development?

- ☐ Involve key stakeholders.
- ☒ Implement project steering committee review.
- ☐ Implement a quality management system.
- ☐ Establish key performance indicators (KPIs).

Question 555

Which of the following stakeholders should be PRIMARILY responsible for developing, implementing, and monitoring metrics for security activities?

- ☒ Chief technology officer
- ☐ Security incident response team
- ☐ Chief information security officer
- ☐ IT steering committee

Question 556

Which of the following is the PRIMARY objective of using a capability maturity model as a tool to communicate audit results to senior management?

- ☒ To evaluate management's action plan
- ☐ To confirm audit findings
- ☐ To illustrate improvement opportunities
- ☐ To prioritize remediation efforts

Question 557

Which of the following is an environmental issue caused by electric storms or noisy electric equipment and may also cause computer system to hang or crash?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☒ EMI

Explanation:

Explanation:

The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

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

Because Unshielded Twisted Pair cables does not have shielding like shielded twisted-pair cables, UTP is susceptible to interference from external electrical sources, which could reduce the integrity of the signal. Also, to intercept transmitted data, an intruder can install a tap on the cable or monitor the radiation from the wire. Thus, UTP may not be a good choice when transmitting very sensitive data or when installed in an environment with much electromagnetic interference (EMI) or radio frequency interference (RFI). Despite its drawbacks, UTP is the most common cable type. UTP is inexpensive, can be easily bent during installation, and, in most cases, the risk from the above drawbacks is not enough to justify more expensive cables.

For your exam you should know below information about power failure

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Sags, spike and surge – Temporary and rapid decreases (sag) or increases (spike and surges) in a voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices.

Electromagnetic interference (EMI) - The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

The following were incorrect answers:

Sag – Temporarily rapid decrease in a voltage.

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

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

Reference:

CISA review manual 2014 Page number372

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 6507-6512). Acerbic Publications. Kindle Edition.

Question 558

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

Question 559

An IS auditor reviews an organizational chart PRIMARILY for:

- ☐ an understanding of workflows.
- ☐ investigating various communication channels.
- ☒ understanding the responsibilities and authority of individuals.
- ☐ investigating the network connected to different employees.

Explanation:

Explanation:

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

Question 560

When determining the specifications for a server supporting an online application using more than a hundred endpoints, which of the following is the MOST important factor to be considered?

- ☐ High availability of different systems
- ☐ Cost-benefit comparison between the available systems
- ☐ Reputation of the vendors and their customer base
- ☒ Transaction volume estimate during peak periods

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

Question 561

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 562

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.

Question 563

A cloud service provider is unable to provide an independent assessment of controls. Which of the following is the BEST way to obtain assurance that the provider can adequately protect the organization's information?

- ☐ Check references supplied by the provider's other customers.
- ☒ Invoke the right to audit per the contract.
- ☐ Review the provider's information security policy.
- ☐ Review the provider's self-assessment.

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

Question 564

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 565

Which of the following should be the FIRST step in the incident response process for a suspected breach?

- ☐ Inform potentially affected customers of the security breach.
- ☐ Notify business management of the security breach.
- ☐ Engage a third party to independently evaluate the alerted breach.
- ☒ Research the validity of the alerted breach.

Question 566

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

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☒ TCP

Explanation:

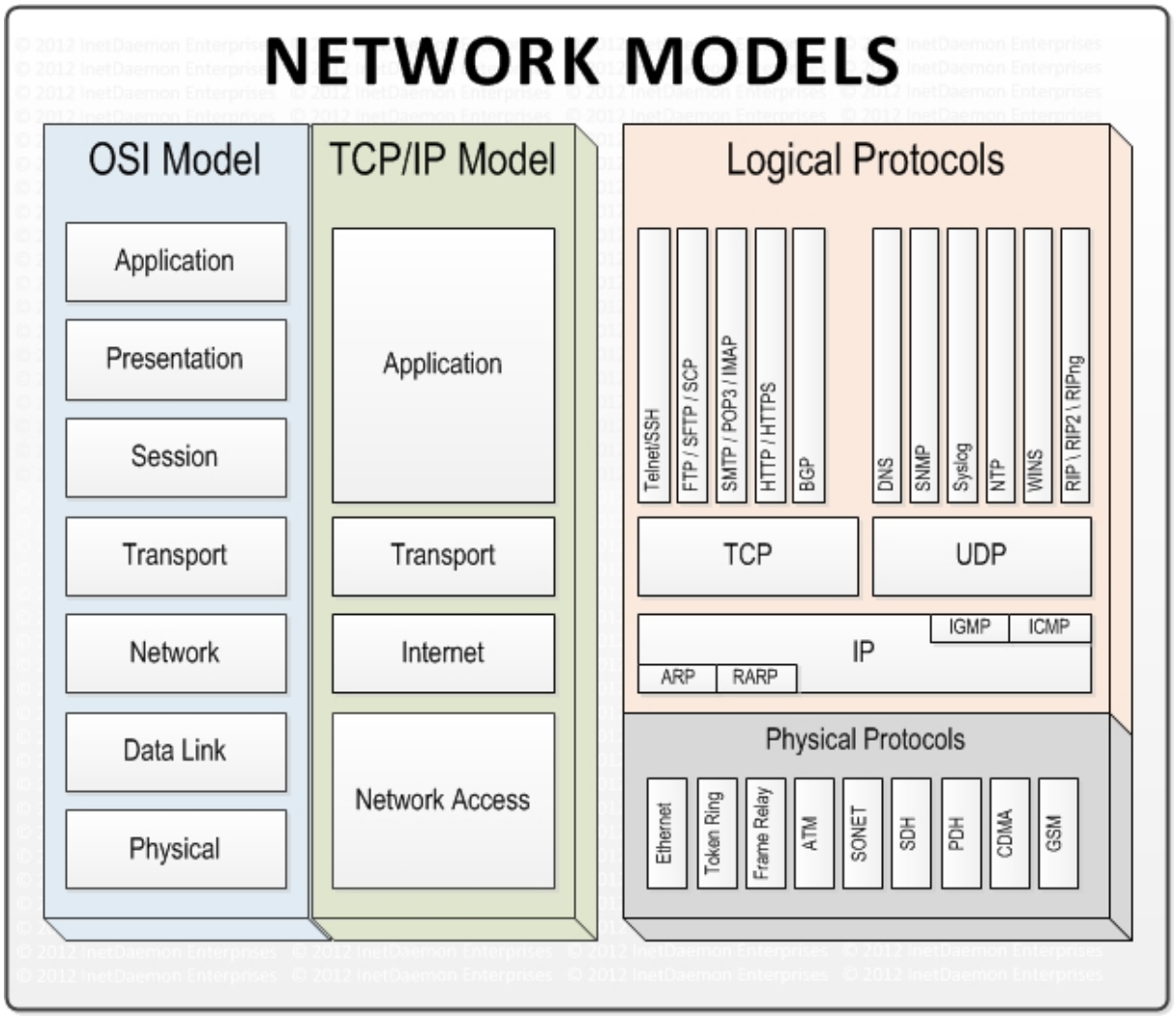
Explanation:

The NOT keyword is used in the question. You need to find out a protocol which does not work at application layer. TCP protocol works at transport layer of a TCP/IP models.

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

Network Models

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



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

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

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

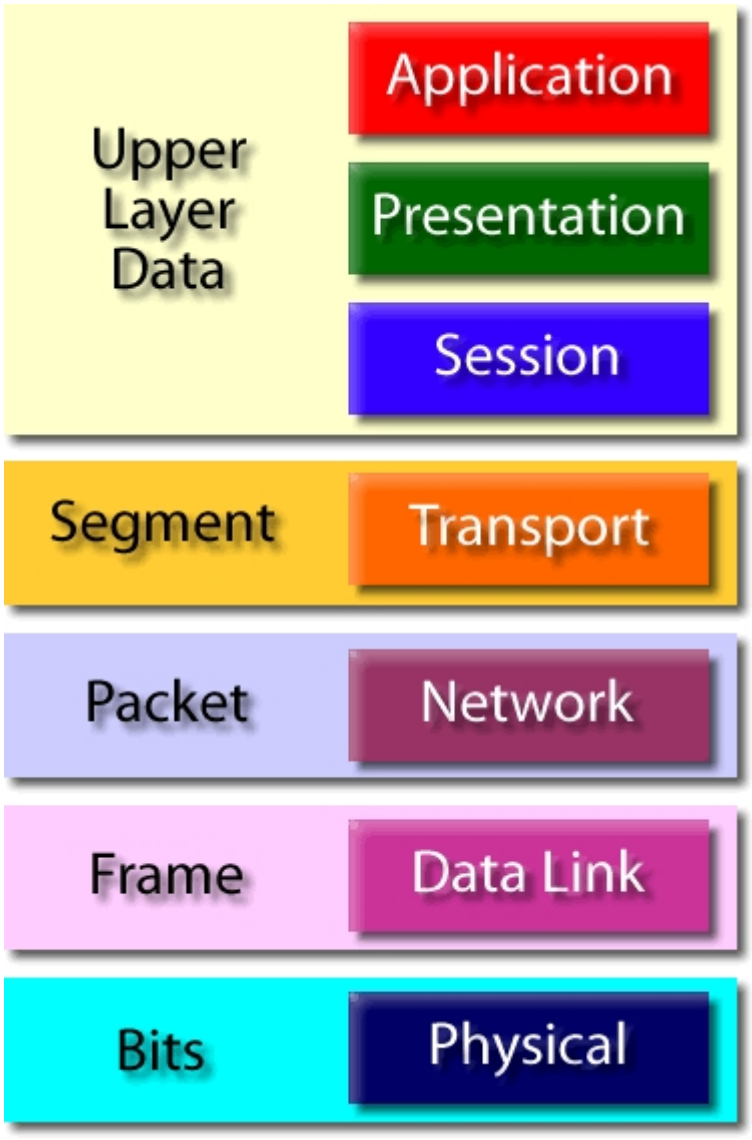
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if

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

two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

HTTP, FTP and NTP protocols works at application layer in TCP/IP model.

Reference:

CISA review manual 2014 page number 272

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

Question 567

The PRIMARY objective of parallel testing an application is to confirm that:

- ☒ the results of calculations in the new system are as accurate as the old system.
- ☐ system response times in the new system are better than the old system.
- ☐ the costs of running the new system are the same as running the old system.
- ☐ new system processing times are similar to those of the old system.

Question 568

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 569

Which of the following is normally a responsibility of the chief security officer (CSO)?

- ☒ Periodically reviewing and evaluating the security policy
- ☐ Executing user application and software testing and evaluation
- ☐ Granting and revoking user access to IT resources
- ☐ Approving access to data and applications

Explanation:

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

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

Question 570

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- ☐ Dumping the memory content to a file
- ☐ Generating disk images of the compromised system
- ☒ Rebooting the system
- ☐ Removing the system from the network

Explanation:

Explanation:

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

Question 571

A financial institution suspects that a manager has been crediting customer accounts without authorization. Which of the following is the MOST effective method to validate this concern?

- ☐ Variable sampling
- ☐ Stop or go sampling
- ☐ Attribute sampling
- ☒ Discovery sampling

Question 572

An organization is considering the implementation of a business application. The IS auditor should FIRST ensure that:

- ☐ user requirements are used to select the vendor.
- ☐ an approved business case is in place.
- ☐ users are represented on the project management team.
- ☒ security requirements are specified.

Question 573

Which of the following audit procedures would be MOST conclusive in evaluating the effectiveness of an e-commerce application system's edit routine?

- ☐ Interviews with knowledgeable users
- ☒ Use of test transactions
- ☐ Review of source code
- ☐ Review of program documentation

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

Question 574

Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

- ☐ Degaussing
- ☒ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Explanation:

Explanation:

Software tools can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media.

For your exam you should know the information below:

When media is to be reassigned (a form of object reuse), it is important that all residual data is carefully removed. Simply deleting files or formatting media does not actually remove the information. File deletion and media formatting often simply remove the pointers to the information. Providing assurance for object reuse requires specialized tools and techniques according to the type of media on which the data resides. Specialized hardware devices known as degausses can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity. It is important to make sure that the coercivity of the degasser is of sufficient strength to meet object reuse requirements when erasing data. If a degasser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over. Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse. Some degausses can destroy drives. The security professional should exercise caution when recommending or using degausses on media for reuse.

Software tools also exist that can provide object reuse assurance. These tools overwrite every sector of magnetic media with a random or predetermined bit pattern. Overwrite methods are effective for all forms of electronic media with the exception of read-only optical media. There exists a drawback to using overwrite software. During normal write operations with magnetic media, the head of the drive moves back-and-forth across the media as data is written. The track of the head does not usually follow the exact path each time. The result is a miniscule amount of data remanence with each pass. With specialized equipment, it is possible to read data that has been overwritten. To provide higher assurance in this case, it is necessary to overwrite each sector multiple times. Security practitioners should keep in mind that a one-time pass may be acceptable for noncritical information, but sensitive data should be overwritten with multiple passes. Overwrite software can also be used to clear the sectors within solid-state media such as USB thumb drives. It is suggested that physical destruction methods such as incineration or secure recycling should be considered for solid-state media that is no longer used.

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

The last form of preventing unauthorized access to sensitive data is media destruction. Shredding, burning, grinding, and pulverizing are common methods of physically destroying media. Degaussing can also be a form of media destruction. High-power degausses are so strong in some cases that they can literally bend and warp the platters in a hard drive. Shredding and burning are effective destruction methods for non-rigid magnetic media. Indeed, some shredders are capable of shredding some rigid media such as an optical disk. This may be an effective alternative for any optical media containing nonsensitive information due to the residue size remaining after feeding the disk into the machine. However, the residue size might be too large for media containing sensitive information. Alternatively, grinding and pulverizing are acceptable choices for rigid and solid-state media. Specialized devices are available for grinding the face of optical media that either sufficiently scratches the surface to render the media unreadable or actually grinds off the data layer of the disk. Several services also exist which will collect drives, destroy them on site if requested and provide certification of completion. It will be the responsibility of the security professional to help, select, and maintain the most appropriate solutions for media cleansing and disposal.

The following answers are incorrect:

Degaussing -Erasing data by applying magnetic field around magnetic media. Degausses device is used to erase the data. Sometime degausses can make magnetic media unusable. So degaussing is not recommended way if magnetic media needs to be reused.

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.

Reference:

CISA review manual 2014 Page number 338

Question 575

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 576

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

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

Question 577

Which of the following is a risk of cross-training?

- ☐ Increases the dependence on one employee
- ☐ Does not assist in succession planning
- ☒ One employee may know all parts of a system
- ☐ Does not help in achieving a continuity of operations

Explanation:

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

Question 578

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:

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:

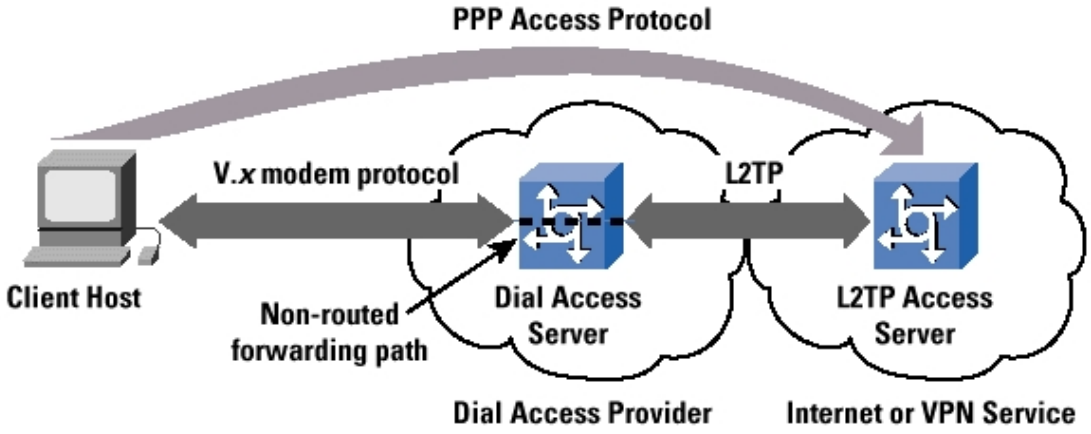
Licensed to Berend Post berend.post@it-university.nl

Point-to-point protocol

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

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

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



Point-to-point protocol

X.25

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

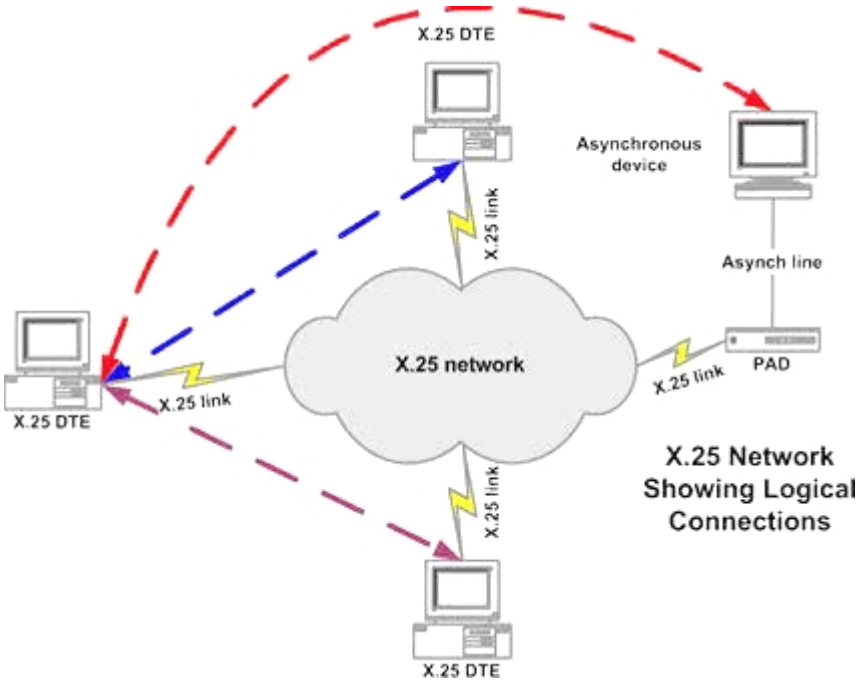
X.25 is a packet switching technology which uses carrier switch to provide connectivity for many different networks.

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

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

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 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.

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

Frame Relay

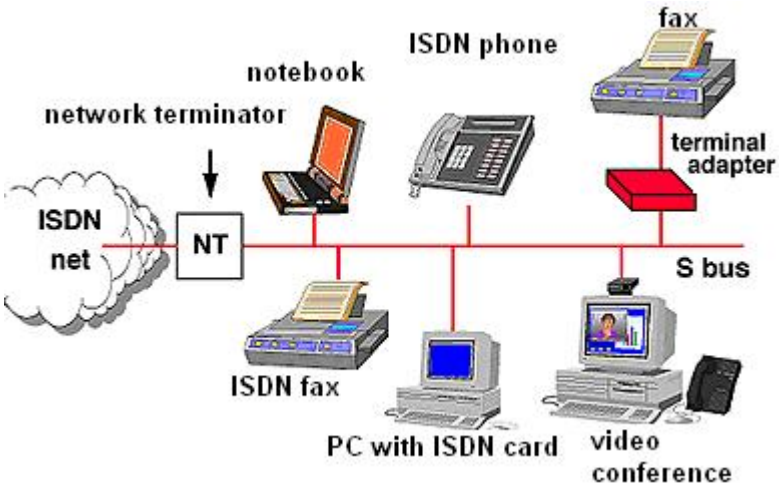
Integrated Service Digital Network

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)

Uses Cell switching method

High speed network technology used for LAN, MAN and WAN

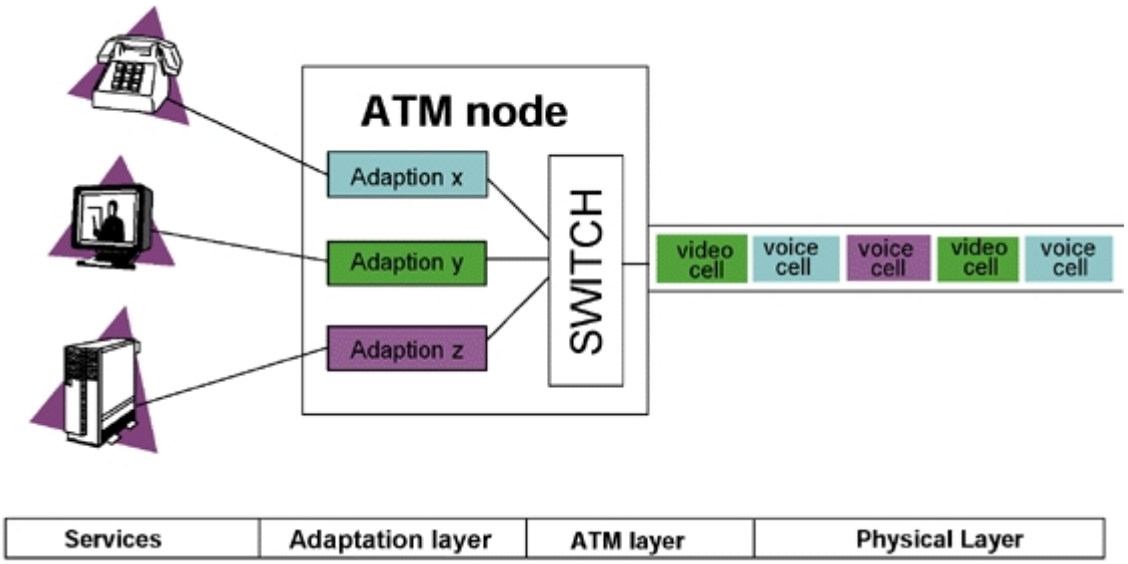
Like a frame relay it is connection oriented technology which creates and uses fixed channel

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

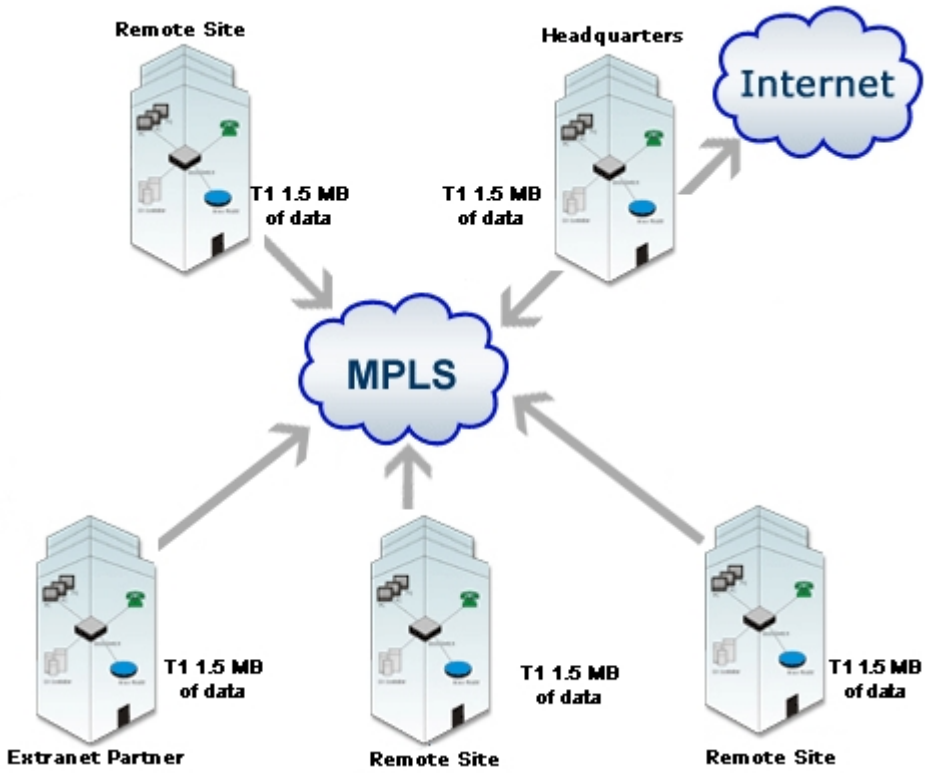


Multiprotocol Label Switching (MPLS)

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

Reference:

CISA review manual 2014 page number 266

Question 579

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- ☒ business plan.
- ☐ audit plan.
- ☐ security plan.
- ☐ investment plan.

Explanation:

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

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.

Question 580

What is the BEST method to determine if IT resource spending is aligned with planned project spending?

- ☒ Earned value analysis (EVA)
- ☐ Gantt chart
- ☐ Return on investment (ROI) analysis
- ☐ Critical path analysis

Question 581

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 582

An organization has replaced all of the storage devices at its primary data center with new, higher capacity units. The replaced devices have been installed at the disaster recovery site to replace older units. An IS auditor's PRIMARY concern would be whether:

- ☒ the procurement was in accordance with corporate policies and procedures
- ☐ the relocation plan has been communicated to all concerned parties
- ☐ a hardware maintenance contract is in place for both old and new storage devices
- ☐ the recovery site devices can handle the storage requirements

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

Question 583

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:

Explanation:

A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

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

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

and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.

Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:

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.

Reference:

CISA review manual 2014 Page number 258

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

Question 584

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 585

TEMPEST is a hardware for which of the following purposes?

- ☒ Eavedropping
- ☐ Social engineering
- ☐ Virus scanning
- ☐ Firewalling
- ☐ None of the choices.

Explanation:

Explanation:

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system can be eavesdropped upon via monitoring the faint electromagnetic transmissions generated by the hardware such as TEMPEST.

Question 586

An IS auditor is reviewing an organization's sales and purchasing system due to ongoing data quality issues. An analysis of which of the following would provide the MOST useful information to determine the revenue loss?

- ☐ Correlation between the number of issues and average downtime
- ☐ Cost of implementing data validation controls within the system
- ☐ Comparison of the cost of data acquisition and loss in sales revenue
- ☒ Correlation between data errors and loss in value of transactions

Question 587

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

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

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

Question 588

Which of the following is the GREATEST advantage of application penetration testing over vulnerability scanning?

- ☐ Penetration testing does not require a special skill set to be executed.
- ☒ Penetration testing provides a more accurate picture of gaps in application controls.
- ☐ Penetration testing can be conducted in a relatively short time period.
- ☐ Penetration testing creates relatively smaller risks to application availability and integrity.

Question 589

When reviewing a contract for a disaster recovery hot site, which of the following would be the MOST significant omission?

- ☐ Audit rights
- ☐ Testing procedures
- ☒ Exposure coverage
- ☐ Equipment provided

Question 590

Controls related to authorized modifications to production programs are BEST tested by:

- ☐ testing only the authorizations to implement the new program.
- ☐ tracing modifications from the executable program back to the original request for change.
- ☐ reviewing only the actual lines of source code changed in the program.
- ☒ tracing modifications from the original request for change forward to the executable program.

Question 591

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

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

unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirement.

Question 592

To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

- ☐ enterprise data model.
- ☒ IT balanced scorecard (BSC).
- ☐ IT organizational structure.
- ☐ historical financial statements.

Explanation:

Explanation:

The IT balanced scorecard (BSC) is a tool that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. An enterprise data model is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity. Historical financial statements do not provide information about planning and lack sufficient detail to enable one to fully understand management’s activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

Question 593

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.

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

Question 594

Which of the following provides the MOST assurance that a newly developed web application does not have IT security issues?

- ☐ Server hardening
- ☐ Business impact analysis (BIA)
- ☐ Application whitelisting
- ☒ Penetration testing

Question 595

During an external assessment of network vulnerability, which of the following activities should be performed FIRST?

- ☒ Collect network information
- ☐ Implement an intrusion detection system (IDS)
- ☐ Monitor the network
- ☐ Review policies

Question 596

Which of the following protocol does NOT work at Network interface layer in TCP/IP model?

- ☐ ICMP
- ☒ DNS
- ☐ ARP
- ☐ Internet protocol

Explanation:

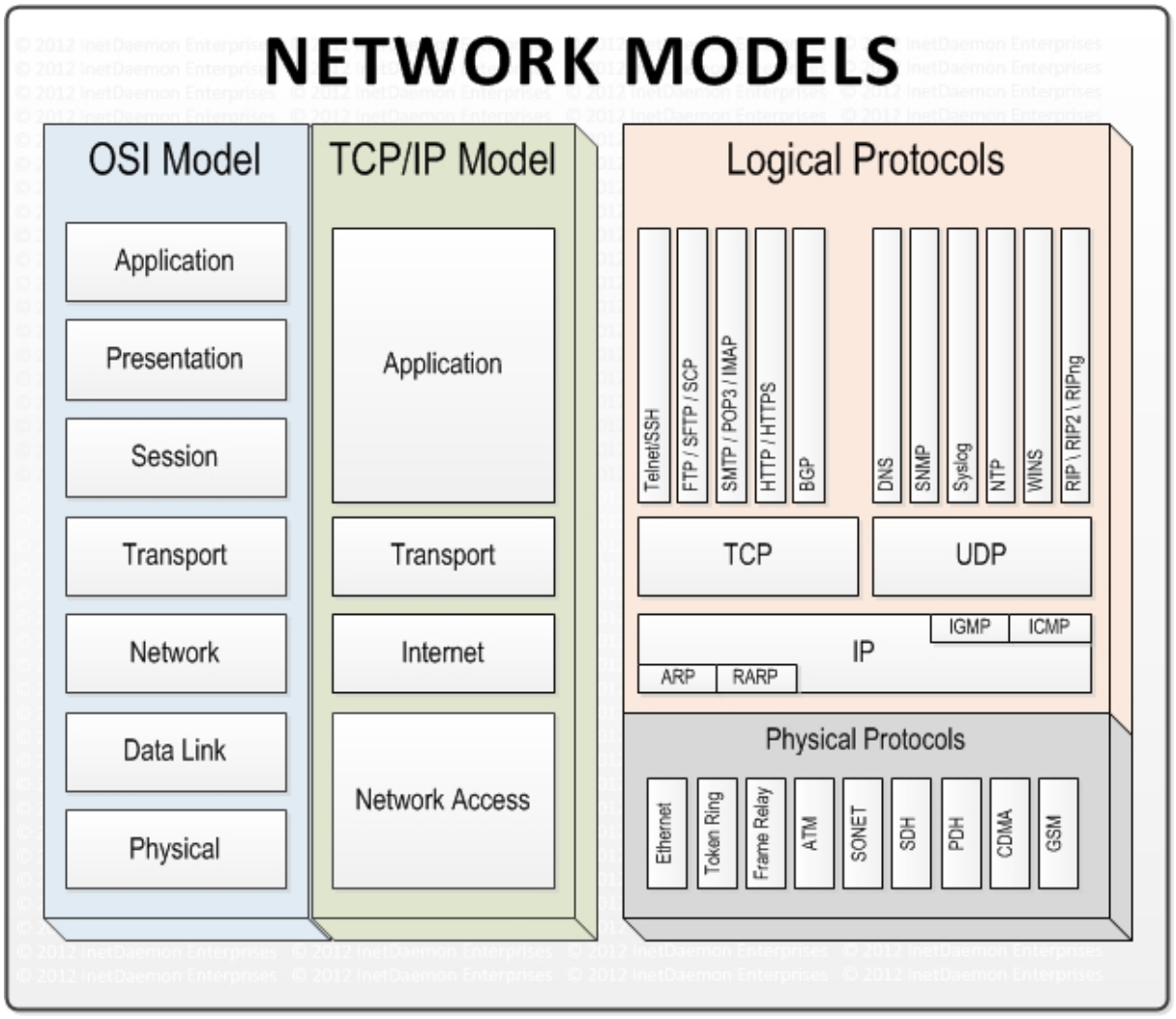
Explanation:

The NOT is the keyword used in the question. You need to find out a protocol which does not work at network interface layer in TCP/IP model. DNS protocol works at application layer of a TCP/IP model.

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

Network models

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.

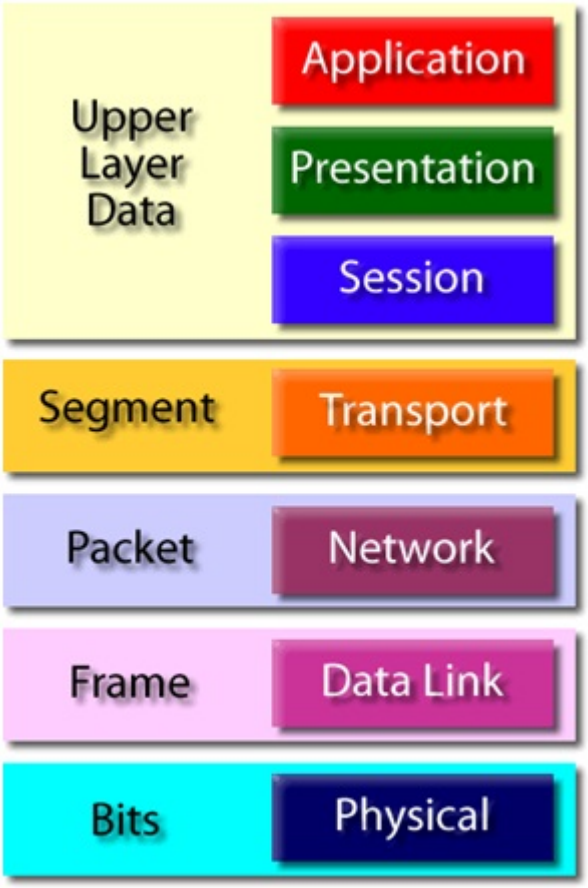
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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):



The following answers are incorrect:

ICMP, ARP and Internet protocol works at Network interface layer of a TCP/IP model.

Reference:

CISA review manual 2014 page number 272

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

Question 597

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

- ☐ record the observations separately with the impact of each of them marked against each respective finding.
- ☐ advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
- ☒ record the observations and the risk arising from the collective weaknesses.
- ☐ apprise the departmental heads concerned with each observation and properly document it in the report.

Explanation:

Explanation:

Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined effect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

Question 598

An IS auditor is reviewing a sample of production incidents and notes that root cause analysis is not being performed. Which of the following is the GREATEST risk associated with this finding?

- ☐ Future incidents may not be resolved in a timely manner.
- ☐ Future incidents may be prioritized inappropriately.
- ☒ The same incident may occur in the future.
- ☐ Service level agreements (SLAs) may not be met.

Question 599

Which of the following is a type of computer network used for data transmission among devices such as computers, telephones and personal digital assistants?

- ☐ LAN
- ☐ WAN
- ☒ SAN
- ☐ PAN

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

Question 600

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 601

A trojan horse simply cannot operate autonomously.

- ☒ true
- ☐ false

Explanation:

Explanation:

As a common type of Trojan horses, a legitimate software might have been corrupted with malicious code which runs when the program is used. The key is that the user has to invoke the program in order to trigger the malicious code. In other words, a trojan horse simply cannot operate autonomously. You would also want to know that most but not all trojan horse payloads are harmful - a few of them are harmless.

Question 602

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:

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.

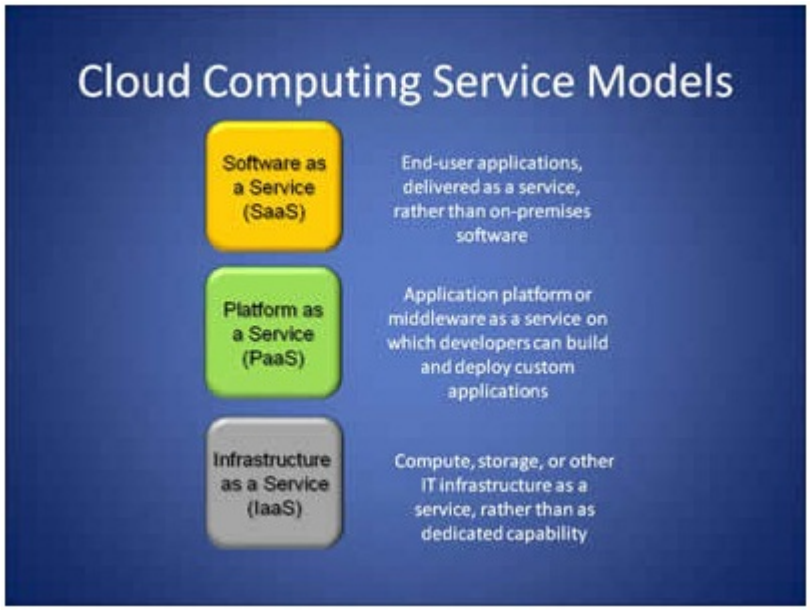
For your exam you should know below information about Cloud Computing:

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 service model

Cloud computing service models



Software as a Service (Seas)

Software as a Service (Seas) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is closely related to the ASP (application service provider) and on demand computing software delivery models. IDC identifies two slightly different delivery models for Seas. The hosted application management (hosted AM) model is similar to ASP: a provider hosts commercially available software for customers and delivers it over the Web. In the software on demand model, the provider gives customers network-based access to a single copy of an application created specifically for Seas distribution.

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 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.

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.

The following answers are incorrect:

Data as a service - Data Provided as a service rather than needing to be loaded and prepared on premises.

Platform as a service - Platform as a Service (Peas) is a way to rent hardware, operating systems, storage and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.

Infrastructure as a service - Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

Reference:

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 603

Which of the following level in CMMI model focuses on process innovation and continuous optimization?

- ☐ Level 4
- ☒ Level 5
- ☐ Level 3
- ☐ Level 2

Explanation:

Explanation:

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

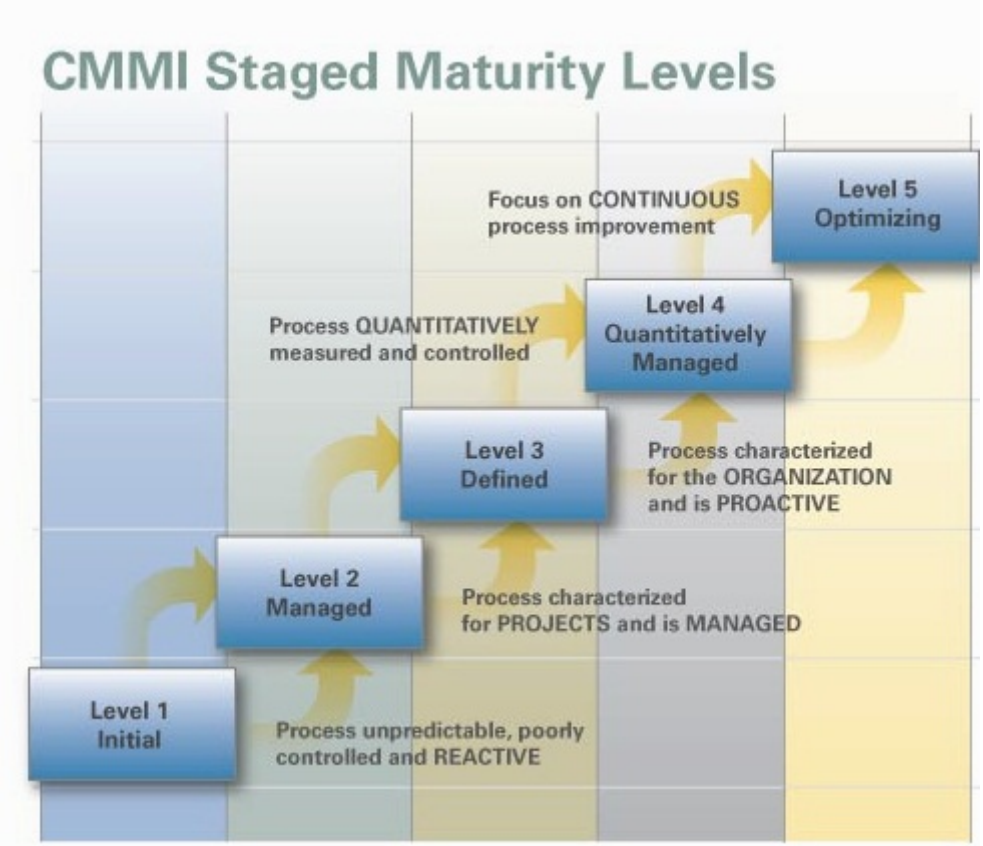
Level 5 is the optimizing process and focus on process innovation and continuous integration.

For CISA Exam you should know below information about Capability Maturity Model Integration (CMMI) mode:

Maturity model

A maturity model can be viewed as a set of structured levels that describe how well the behaviors, practices and processes of an organization can reliably and sustainable produce required outcomes.

CMMI Levels



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

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

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".[citation needed]

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

Repeatable - the process is at least documented sufficiently such that repeating the same steps may be attempted.

Defined - the process is defined/confirmed as a standard business process, and decomposed to levels 0, 1 and 2 (the last being Work Instructions).

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.

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

These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

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.

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

The following were incorrect answers:

Level 4 – Focus on process management and process control

Level 3 – Process definition and process deployment.

Level 2 – Performance management and work product management.

Reference:

CISA review manual 2014 Page number 188

Question 604

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

- ☐ Business interruption
- ☒ Fidelity coverage
- ☐ Errors and omissions
- ☐ Extra expense

Explanation:

Explanation:

Fidelity insurance covers the loss arising from dishonest or fraudulent acts by employees. Business interruption insurance covers the loss of profit due to the disruption in the operations of an organization. Errors and omissions insurance provides legal liability protection in the event that the professional practitioner commits an act that results in financial loss to a client. Extra expense insurance is designed to cover the extra costs of continuing operations following a disaster/disruption within an organization.

Question 605

Assessing IT risks is BEST achieved by:

- ☒ evaluating threats associated with existing IT assets and IT projects.
- ☐ using the firm's past actual loss experience to determine current exposure.
- ☐ reviewing published loss statistics from comparable organizations.
- ☐ reviewing IT control weaknesses identified in audit reports.

Explanation:

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not

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

adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

Question 606

During an audit of the organization's data privacy policy, the IS auditor identified that only some IT application databases have encryption in place. What should be the auditor's FIRST action?

- ☐ Assess the resources required to implement encryption to unencrypted databases.
- ☐ Review the most recent database penetration testing results.
- ☒ Determine whether compensating controls are in place.
- ☐ Review a comprehensive list of databases with the information they contain.

Question 607

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 608

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

- ☒ Blackbox test
- ☐ Desk checking
- ☐ Structured walk-through
- ☐ Design and code

Explanation:

Explanation:

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules, a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

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

Question 609

Which of the following reduces the potential impact of social engineering attacks?

- ☐ Compliance with regulatory requirements
- ☐ Promoting ethical understanding
- ☒ Security awareness programs
- ☐ Effective performance incentives

Explanation:

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

Question 610

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

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

Question 611

Which of the following would MOST effectively detect a condition where an employee assigned to an operations role could perform system administrator functions?

- ☒ User access review
- ☐ System review
- ☐ Business process review
- ☐ Entitlement design review

Question 612

Which of the following is the BEST way to determine the effectiveness of a recently installed intrusion detection system (IDS)?

- ☐ Implement access control.
- ☒ Conduct attack simulation.
- ☐ Review audit logs.
- ☐ Inspect IDS configuration.

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

Question 613

Which of the following should be of MOST concern to an IS auditor evaluating a forensics program?

- ☐ Forensic images are stored on removable media with encryption.
- ☐ Forensic images are only stored for involuntarily terminated employees.
- ☐ Forensic images are only maintained for 12 months.
- ☒ Forensic images are stored on shared disks.

Question 614

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 615

An information systems security officer's PRIMARY responsibility for business process applications is to:

- ☐ create role-based rules for each business process.
- ☒ ensure access rules agree with policies.
- ☐ authorize secured emergency access.
- ☐ approve the organization's security policy.

Question 616

Which of the following is the MOST effective control in an organization to mitigate the risk of insider misuse of personal devices?

- ☐ Security risk assessments
- ☐ Periodic vulnerability scanning
- ☐ Security awareness training
- ☒ Comprehensive procedures on data security

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

Question 617

An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

- ☐ Permanent table-space allocation
- ☐ Commitment and rollback controls
- ☒ User spool and database limit controls
- ☐ Read/write access log controls

Explanation:

Explanation:

User spool limits restrict the space available for running user queries. This prevents poorly formed queries from consuming excessive system resources and impacting general query performance. Limiting the space available to users in their own databases prevents them from building excessively large tables. This helps to control space utilization which itself acts to help performance by maintaining a buffer between the actual data volume stored and the physical device capacity. Additionally, it prevents users from consuming excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run overnight and are optimized for performance purposes), in a data warehouse, since you are not running online transactions, commitment and rollback does not have an impact on performance. The other choices are not as likely to be the root cause of this performance issue.

Question 618

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.

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

Question 619

Which of the following is the MOST effective approach for integrating security into application development?

- ☐ Including security in user acceptance testing sign-off
- ☐ Performing vulnerability scans
- ☐ Developing security models in parallel
- ☒ Defining security requirements

Question 620

A user of a telephone banking system has forgotten his personal identification number (PIN). After the user has been authenticated, the BEST method of issuing a new PIN is to have:

- ☒ the user enter a new PIN twice.
- ☐ banking personnel verbally assign a new PIN.
- ☐ a randomly generated PIN communicated by banking personnel.
- ☐ banking personnel assign the user a new PIN via email.

Question 621

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:

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.

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

2. Contextual and Representational Quality – The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, reorganizing that information quality depends on the context of use. It includes

Relevancy – The extent to which information is applicable and helpful for the task at hand.

Completeness – The extent to which information is not missing and is of sufficient depth and breadth for the task at hand

Currency – The extent to which information is sufficiently up to date for task at hand.

Appropriate amount of information – The extent to which the volume of information is appropriate for the task at hand

Consistent Representation – The extent to which information is presented in the same format.

Interpretability – The extent to which information is in appropriate languages, symbols and units, with clear definitions.

Understandability - The extent to which information is easily comprehended.

Ease of manipulation – The extent to which information is easy to manipulate and apply to different tasks.

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.

Reference:

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

CISA review manual 2014 Page number 310

Question 622

An organization has implemented data storage hardware. Which of the following should an IS auditor review to assess if IT is maximizing storage and network utilization?

- ☒ Capacity management plans
- ☐ Downtime statistics
- ☐ The quality management systems
- ☐ Routine and non-routine job schedules

Question 623

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

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

Explanation:

Explanation:

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

Question 624

Which of the following layer of an enterprise data flow architecture does the scheduling of the tasks necessary to build and maintain the Data Warehouse (DW) and also populates Data Marts?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☒ Warehouse management layer
- ☐ Data access layer

Explanation:

Explanation:

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

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

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

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

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

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

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Desktop access layer or presentation layer is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Data access layer – his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Reference:

CISA review manual 2014 Page number 188

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

Question 625

Which of the following is the BEST methodology to use for estimating the complexity of developing a large business application?

- ☒ Function point analysis
- ☐ Software cost estimation
- ☐ Work breakdown structure
- ☐ Critical path analysis

Question 626

Which of the following is the GREATEST security threat when an organization allows remote access to a virtual private network (VPN)?

- ☐ Client logins are subject to replay attack.
- ☐ VPN traffic could be sniffed and captured.
- ☒ Compromised VPN clients could impact the network.
- ☐ Attackers could compromise the VPN gateway.

Question 627

When are benchmarking partners identified within the benchmarking process?

- ☐ In the design stage
- ☐ In the testing stage
- ☒ In the research stage
- ☐ In the development stage

Explanation:

Explanation:

Benchmarking partners are identified in the research stage of the benchmarking process.

Question 628

In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

- ☐ isolation.
- ☐ consistency.
- ☒ atomicity.
- ☐ durability.

Explanation:

Explanation:

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

The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the database be maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions; hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

Question 629

Which cloud deployment model is MOST likely to be limited in scalability?

- ☐ Public
- ☒ Private
- ☐ Hybrid
- ☐ Community

Question 630

The PRIMARY benefit to using a dry-pipe fire-suppression system rather than a wet-pipe system is that a dry-pipe system:

- ☒ has a decreased risk of leakage.
- ☐ is more effective at suppressing flames.
- ☐ allows more time to abort release of the suppressant.
- ☐ disperses dry chemical suppressants exclusively.

Question 631

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

- ☐ Define the recovery point objective (RPO).
- ☐ Analyze vulnerabilities.
- ☐ Confirm control effectiveness.
- ☒ Determine recovery priorities.

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

Question 632

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

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

Question 633

The members of an emergency incident response team should be:

- ☒ selected from multiple departments
- ☐ assigned at the time of each incident
- ☐ restricted to IT personnel
- ☐ appointed by the CISO

Question 634

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 635

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

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

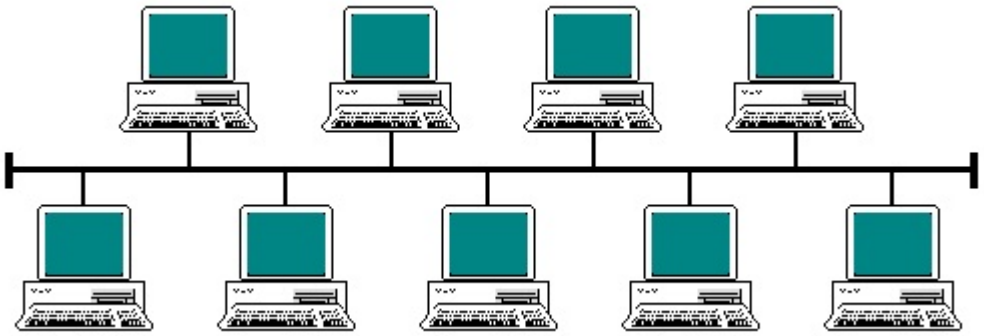
Question 636

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 637

Identify the LAN topology from below diagram presented below:



bus topology

- ☒ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Explanation:

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.

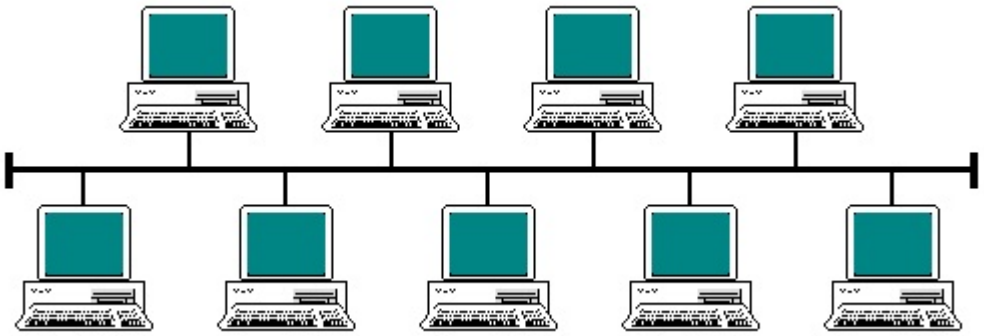
Licensed to Berend Post berend.post@it-university.nl

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

Bus

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology



Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly the same fashion as the physical linear bus topology (i.e., all nodes share a common transmission medium).

Star

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

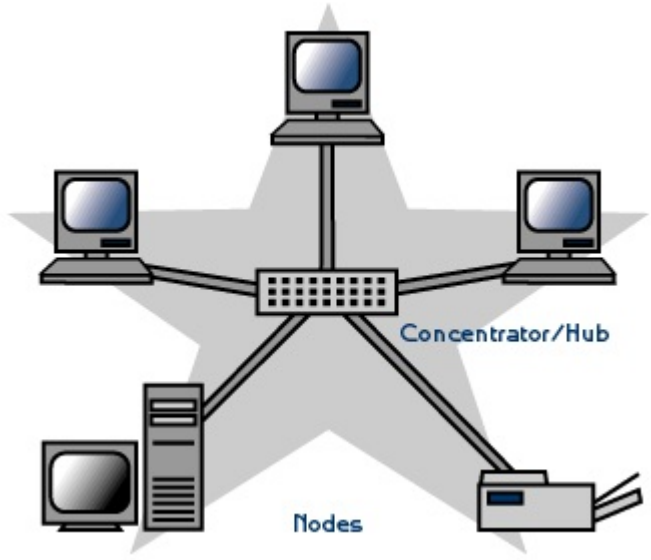
In local area networks with a star topology, each network host is connected to a central point with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch.

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



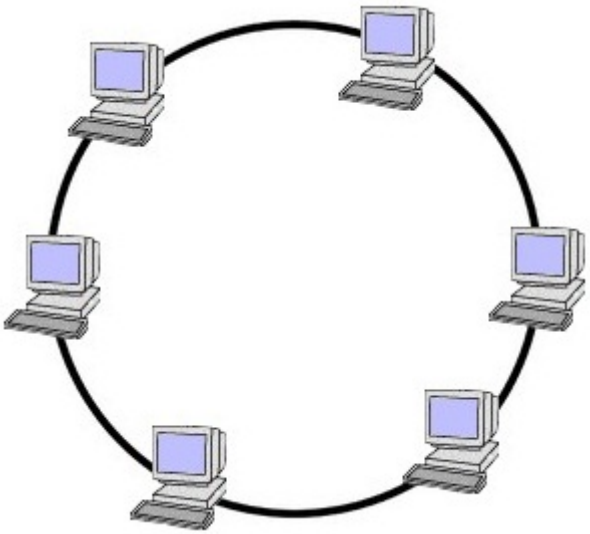
Ring

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.

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.

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

Ring Topology

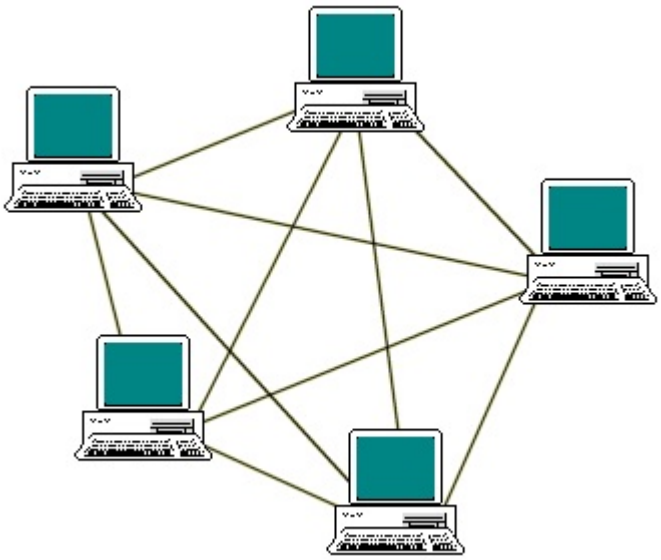


Mesh

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.

Reference:

CISA review manual 2014, Page number 262

Question 638

In a decentralized organization, the selection and purchase of IS products is acceptable as long as which of the following conditions exists?

- ☐ The same operating system is used throughout the organization.
- ☐ Various offices are independent and exchange data on an occasional basis.
- ☒ Acquired items are consistent with the organization's short- and long-term IS strategy plans.
- ☐ Managers undertake a full cost-benefit analysis before deciding what to purchase.

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

Question 639

Which of the following type of network service is used by network computer to obtain an IP addresses and other parameters such as default gateway, subnet mask?

- ☒ DHCP
- ☐ DNS
- ☐ Directory Service
- ☐ Network Management

Explanation:

Explanation:

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

For your exam you should know below information about network services:

In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.

Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client 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

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

dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

Network Management - In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

Dynamic Host Configuration Protocol (DHCP) - The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

Email service - Provides the ability, through a terminal or PC connected to a communication network, to send an entrusted message to another individual or group of people.

Print Services - Provide the ability, typically through a print server on a network, to manage and execute print request services from other devices on the network

Domain Name System(DNS) - Translates the names of network nodes into network IP address.

The following were incorrect answers:

Directory Service - A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows the lookup of values given a name, similar to a dictionary. As a word in a dictionary may have multiple definitions, in a directory, a name may be associated with multiple, different pieces of information. Likewise, as a word may have different parts of speech and different definitions, a name in a directory may have many different types of data.

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.

Reference:

CISA review manual 2014 Page number 258

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

Question 640

An IS auditor notes that the anticipated benefits from an ongoing infrastructure project have changed due to recent organizational restructuring. Which of the following is the IS auditor's BEST recommendation?

- ☐ Review and reapprove the business case.
- ☒ Revise business goals and objectives.
- ☐ Conduct a new feasibility study.
- ☐ Review and update the business impact analysis (BIA).

Question 641

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 642

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

- ☐ interface errors are detected earlier.
- ☐ confidence in the system is achieved earlier.
- ☒ errors in critical modules are detected earlier.
- ☐ major functions and processing are tested earlier.

Explanation:

Explanation:

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach, which follows the opposite path, either in depth-first or breadth-first search order.

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

Question 643

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 644

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 645

The IS auditor of a power company finds that the radio link to a remote mountain site is experiencing systematic outages under specific weather conditions. The communications manager explains that increasing the radio power would require a new license and would help little. What is the MOST appropriate action by the IS auditor?

- ☐ Recommend that the site's data collection and transmission be non-interruptible.
- ☐ Review the installation license, permissions and associated costs.
- ☐ Recommend that the site's hardware be upgraded to record data during outages.
- ☒ Gather additional information to identify threats, vulnerabilities, and impact.

Question 646

Information for detecting unauthorized input from a terminal would be BEST provided by the:

- ☐ console log printout.
- ☒ transaction journal.
- ☐ automated suspense file listing.
- ☐ user error report.

Explanation:

Explanation:

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing

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

would only list transaction activity where an edit error occurred, while the user error report would only list input that resulted in an edit error.

Question 647

If the recovery time objective (RTO) increases:

- ☒ the disaster tolerance increases.
- ☐ the cost of recovery increases.
- ☐ a cold site cannot be used.
- ☐ the data backup frequency increases.

Explanation:

Explanation:

The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

Question 648

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- ☐ Paper test
- ☐ Post test
- ☒ Preparedness test
- ☐ Walk-through

Explanation:

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. A paper test is a walkthrough of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution. A paper test usually precedes the preparedness test. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third- party systems. A walkthrough is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

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

Question 649

Which of the following would be MOST useful for determining whether the goals of IT are aligned with the organization's goals?

- ☒ Balanced scorecard
- ☐ Enterprise architecture
- ☐ Key performance indicators
- ☐ Enterprise dashboard

Question 650

Which of the following is the FIRST consideration when developing a data retention policy?

- ☐ Determining the backup cycle based on retention period
- ☐ Designing an infrastructure storage strategy
- ☐ Identifying the legal and contractual retention period for data
- ☒ Determining the security access privileges to the data

Question 651

An IS auditor observed that most users do not comply with physical access controls. The business manager has explained that the control design is inefficient. What is the auditor's BEST course of action?

- ☐ Recommend changing the access control process to increase efficiency.
- ☐ Identify the impact of control failure and report the finding with a risk rating.
- ☒ Redesign and retest the physical access control.
- ☐ Work with management to design and implement a better control.

Question 652

An IS auditor has completed an audit on the organization's IT strategic planning process. Which of the following findings should be given the HIGHEST priority?

- ☒ The IT strategic plan was completed prior to the formulation of the business strategic plan
- ☐ Assumptions in the IT strategic plan have not been communicated to business stakeholders
- ☐ The IT strategic plan was formulated based on the current IT capabilities
- ☐ The IT strategic plan does not include resource requirements for implementation

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

Question 653

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.

Question 654

An IS auditor selects a server for a penetration test that will be carried out by a technical specialist. Which of the following is MOST important?

- ☐ The tools used to conduct the test
- ☐ Certifications held by the IS auditor
- ☒ Permission from the data owner of the server
- ☐ An intrusion detection system (IDS) is enabled

Explanation:

Explanation:

The data owner should be informed of the risks associated with a penetration test, what types of tests are to be conducted and other relevant details. All other choices are not as important as the data owner's responsibility for the security of the data assets.

Question 655

An IS auditor suspects an organization's computer may have been used to commit a crime. Which of the following is the auditor's BEST course of action?

- ☐ Examine the computer to search for evidence supporting the suspicions.
- ☐ Notify local law enforcement of the potential crime before further investigation.
- ☒ Contact the incident response team to conduct an investigation.
- ☐ Advise management of the crime after the investigation.

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

Question 656

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 657

The responsibilities of a disaster recovery relocation team include:

- ☐ obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
- ☐ locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
- ☐ managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
- ☒ coordinating the process of moving from the hot site to a new location or to the restored original location.

Explanation:

Explanation:

Choice A describes an offsite storage team, choice B defines a transportation team and choice C defines a salvage team.

Question 658

Using swipe cards to limit employee access to restricted areas requires implementing which additional control?

- ☒ Physical sign-in of all employees for access to restricted areas
- ☐ Initial escort of all new hires by a current employee
- ☐ Periodic review of access profiles by management
- ☐ Employee-access criteria determined on the basis of IS experience

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

Question 659

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

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

Explanation:

Explanation:

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

Question 660

Which of the following is an effective method for controlling downloading of files via FTP?

- ☐ An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
- ☒ An application-layer gateway, or proxy firewall
- ☐ A circuit-level gateway
- ☐ A first-generation packet-filtering firewall

Explanation:

Explanation:

Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

Question 661

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 662

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 663

When reviewing backup policies, an IS auditor MUST verify that backup intervals of critical systems do not exceed which of the following?

- ☒ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)
- ☐ Service level objective (SLO)
- ☐ Maximum acceptable outage (MAO)

Question 664

Which of the following statement is NOT true about smoke detector?

- ☐ The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
- ☐ The smoke detector should produce an audible alarm when activated and be linked to a monitored station
- ☐ The location of the smoke detector should be marked on the tiling for easy identification and access
- ☒ Smoke detector should replace fire suppression system

Explanation:

Explanation:

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

The word NOT is the keyword used in the question. You need to find out a statement which is not applicable to smoke detector. Smoke detector should supplement, not replace, fire suppression system.

For CISA exam you should know below information about smoke detector.

The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor.

The smoke detector should produce an audible alarm when activated be linked to a monitored station

The location of the smoke detector should be marked on the tiling for easy identification and access.

Smoke detector should supplement, not replace, fire suppression system

The following were incorrect answers:

The other presented options are valid statement about smoke detector.

Reference:

CISA review manual 2014 Page number373

Question 665

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:

Explanation:

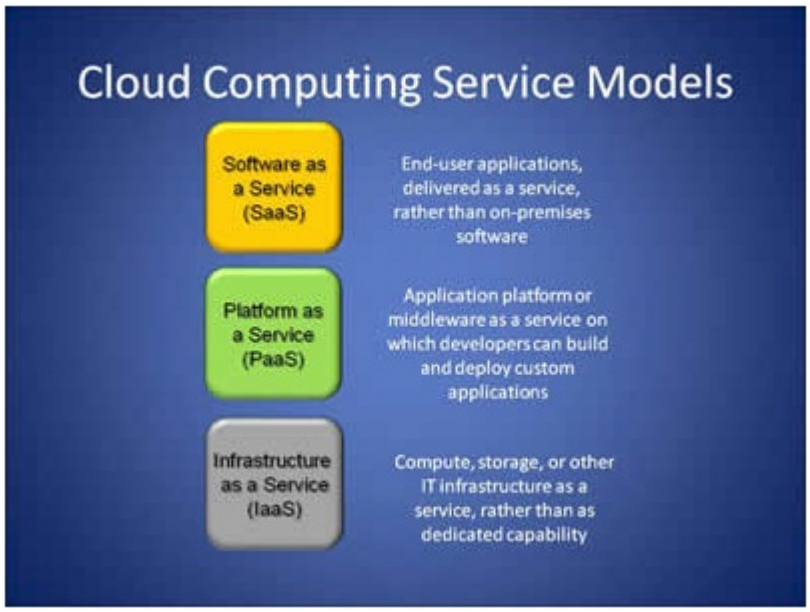
Infrastructure as a Service is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers and networking components. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis.

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

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

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud Computing



Cloud computing service models:

Cloud computing service models

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 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.

 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.

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.

Reference:

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

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 666

The MOST appropriate person to chair the steering committee for an enterprise-wide system development should normally be the:

- ☐ project manager
- ☐ IS director
- ☒ executive level manager.
- ☐ business analyst

Question 667

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

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

Explanation:

Explanation:

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

Question 668

Management has decided to include a compliance manager in the approval process for a new business that may require changes to the IT infrastructure. Which of the following is the GREATEST benefit of this approach?

- ☐ Security breach incidents can be identified in early stages.
- ☒ Regulatory risk exposures can be identified before they materialize.
- ☐ Fewer reviews are needed when updating the IT compliance process.
- ☐ Process accountabilities to external stakeholders are improved.

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

Question 669

An external audit team is deciding whether to rely on internal audit's work for an annual compliance audit. Which of the following is the GREATEST consideration when making this decision?

- ☒ Independence of the internal audit department from management's influence
- ☐ Professional certifications held by the internal audit team members
- ☐ Years of experience each of the internal auditors have in performing compliance audits
- ☐ The level of documentation maintained by internal audit and the methods used to collect evidence

Question 670

Which of the following would be the MOST effective method for detecting duplicate payments?

- ☐ Enciphering and deciphering the message digest
- ☒ Reviewing sequence numbers and time stamps for each transaction
- ☐ Assessing payment history for reasonableness and approval
- ☐ Using a cryptographic hashing algorithm

Question 671

When initiating an IT project, which of the following should be completed FIRST?

- ☐ Project plan
- ☐ Request for proposal
- ☒ Feasibility study
- ☐ Requirements definition

Question 672

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- ☐ Palm scan
- ☐ Face recognition
- ☒ Retina scan
- ☐ Hand geometry

Explanation:

Explanation:

Retina scan uses optical technology to map the capillary pattern of an eye's retina. This is highly reliable and has the lowest false-acceptance rate (FAR) among the current biometric methods. Use of palm scanning entails placing a hand on a scanner where a palm's physical characteristics are captured. Hand geometry, one of the oldest techniques, measures the physical characteristics of the user's hands and fingers from a three dimensional perspective. The palm and hand biometric techniques lack uniqueness in the geometry data. In face biometrics, a reader analyzes the images captured for general facial characteristics. Though considered a natural and friendly biometric, the

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

main disadvantage of face recognition is the lack of uniqueness, which means that people looking alike can fool the device.

Question 673

Which of the following is the BEST way to improve the timely reporting of information security incidents?

- ☐ Perform periodic simulations with the incident response team.
- ☐ Incorporate security procedures in help desk processes.
- ☐ Integrate an intrusion detection system (IDS) in the DMZ.
- ☒ Regularly reassess and update the incident response plan.

Question 674

A bank is relocating its servers to a vendor that provides data center hosting services to multiple clients. Which of the following controls would restrict other clients from physical access to the bank's servers?

- ☐ Closed-circuit television cameras
- ☒ Locking server cages
- ☐ Biometric access at all data center entrances
- ☐ 24-hour security guards

Question 675

Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

- ☐ A hot site contracted and available as needed.
- ☐ A business continuity manual is available and current.
- ☐ insurance coverage is adequate and premiums are current.
- ☒ Media backups are performed on a timely basis and stored offsite.

Explanation:

Explanation:

Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

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

Question 676

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

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

Question 677

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 678

In a botnet, mailbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

- ☒ Chat system
- ☐ SMS system
- ☐ Email system
- ☐ Log system
- ☐ Kernel system
- ☐ None of the choices.

Explanation:

Explanation:

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware or mailbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

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

Question 679

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 680

What is the PRIMARY purpose of audit trails?

- ☐ To document auditing efforts
- ☐ To correct data integrity errors
- ☒ To establish accountability and responsibility for processed transactions
- ☐ To prevent unauthorized access to data

Explanation:

Explanation:

The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

Question 681

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:

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).

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

The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Reference:

CISA review manual 2014 Page number 322

Question 682

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

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

Question 683

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:

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

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 684

Which of the following INCORRECTLY describes the layer function of the Application Layer within the TCP/IP model?

- ☐ Provides user interface
- ☐ Perform data processing such as encryption, encoding, etc
- ☒ Provides reliable delivery
- ☐ Keeps separate the data of different applications

Explanation:

Explanation:

The word INCORRECTLY keyword is used in the question.

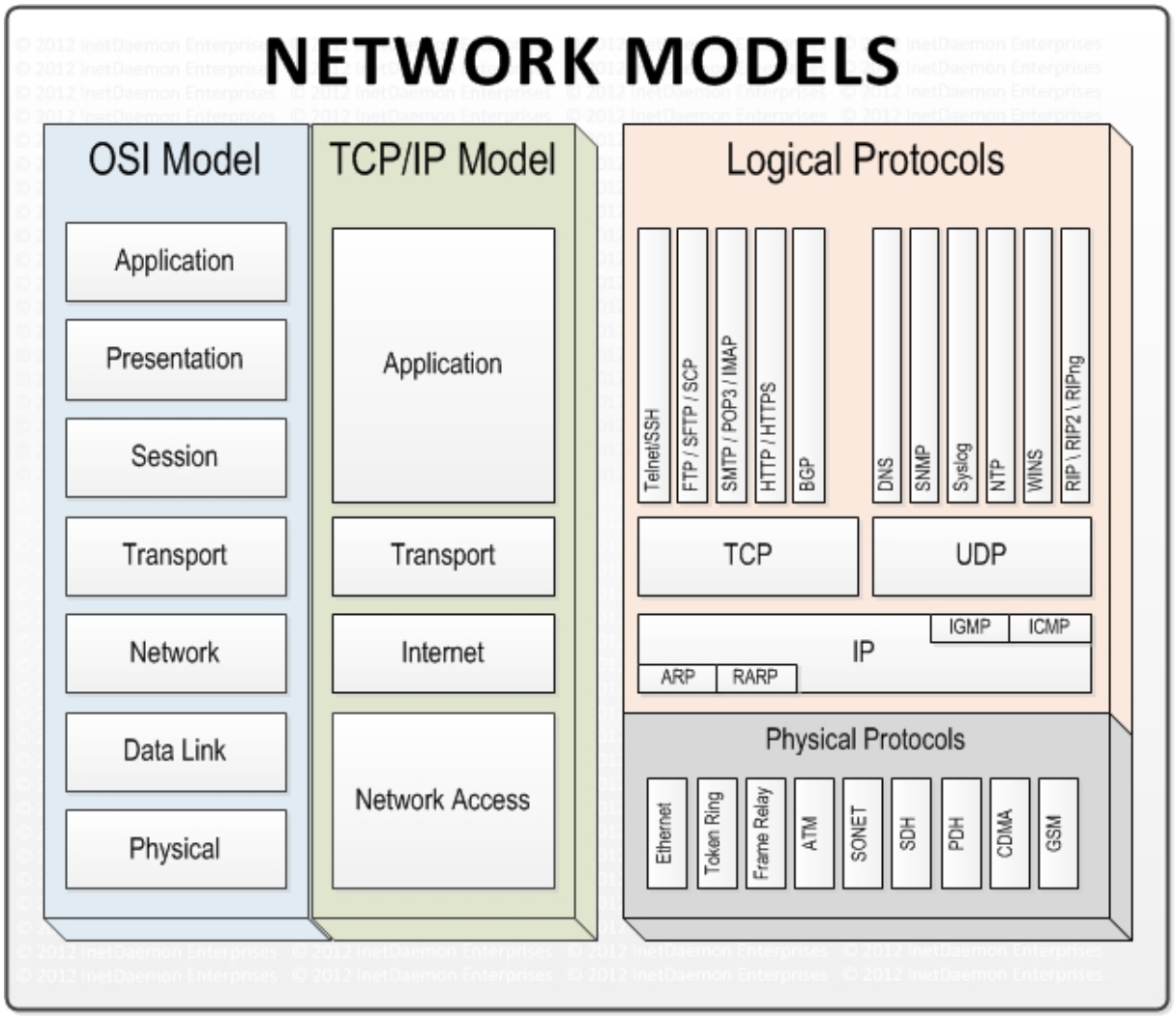
You need to find out the service or functionality which is not performed by application layer of a TCP/IP model.

The reliable or unreliable delivery of a message is the functionality of transport layer of a TCP/IP model.

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

Network Models

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.

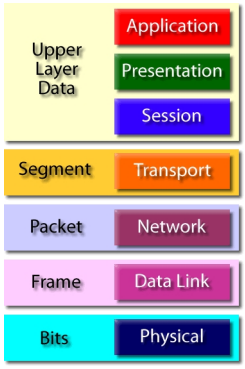
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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):



The following answers are incorrect:

The other options correctly describe functionalities of application layer in TCP/IP model.

Reference:

CISA review manual 2014 page number 272

Question 685

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.

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

Question 686

The PRIMARY purpose of a periodic threat and risk assessment report to senior management is to communicate the:

- ☐ cost-benefit of security controls.
- ☒ status of the security posture.
- ☐ probability of future incidents.
- ☐ risk acceptance criteria.

Question 687

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

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☒ SMTP

Explanation:

Explanation:

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

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

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

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

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

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

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

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

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

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates 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.

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

The following answers are incorrect:

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

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

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

Reference:

CISA review manual 2014 page number 273 and 274

Question 688

Which of the following is the PRIMARY reason social media has become a popular target for attack?

- ☒ The accessibility of social media from multiple locations
- ☐ The prevalence of strong perimeter protection
- ☐ The reduced effectiveness of access controls
- ☐ The element of trust created by social media

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

Question 689

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:

Explanation:

The word NOT the keyword used in the question. You need to find out the technique which preacher do not use to exploit PBX.

SYN Flood -Sends a flood of TCP/SYN packets with forged sender address, causing half-open connections and saturates available connection capacity on the target machine.

For CISA Exam you should know below mentioned techniques used by preacher for illegal purpose of PBX.

Eavesdropping on conversation, without the other parties being aware of it

Eavesdropping on conference call

Illegal forwarding calls from specific equipment to remote numbers

Forwarding a user to an unused or disabled number, thereby making it unreachable by external calls.

The following were incorrect answers:

The other options presented correctly describes the techniques used preacher for illegal purpose of PBX.

Reference:

CISA review manual 2014 Page number 357

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

Question 690

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 691

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 692

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.

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

Question 693

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.

Question 694

An IS auditor finds that a required security patch was not installed on a critical server for more than 6 months. The NEXT course of action should be to:

- ☐ determine the root cause of the delay.
- ☒ review patch management procedures.
- ☐ request the patch be installed as soon as possible.
- ☐ notify senior management of audit findings.

Question 695

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.

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

Question 696

Which of the following is MOST important for an IS auditor to evaluate when determining the effectiveness of an information security program?

- ☐ Percentage of users aware of the objectives of the security program
- ☐ Percentage of policy exceptions that were approved with justification
- ☒ Percentage of desired control objectives achieved
- ☐ Percentage of reported security incidents

Question 697

When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?

- ☐ Report distribution
- ☐ Encryption
- ☒ Tuning
- ☐ Retention

Question 698

Which of the following IS audit recommendations would BEST help to ensure appropriate mitigation will occur on control weaknesses identified during an audit?

- ☒ Assign actions to responsible personnel and follow up.
- ☐ Report on progress to the audit committee.
- ☐ Perform a cost-benefit analysis on remediation strategy.
- ☐ Implement software to input the action points from the IS audit.

Question 699

Outsourcing the development of business systems is MOST likely to result in the loss of:

- ☒ control over strategic direction.
- ☐ accountability for end products.
- ☐ in-house competencies.
- ☐ responsibility for IT security.

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

Question 700

An internal control audit has revealed a control deficiency related to a legacy system where the compensating controls no longer appear to be effective. Which of the following would BEST help the information security manager determine the security requirements to resolve the control deficiency?

- ☐ Cost-benefit analysis
- ☒ Gap analysis
- ☐ Risk assessment
- ☐ Business case

Question 701

An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

- ☒ reduces the risk of unauthorized access to the network.
- ☐ is not suitable for small networks.
- ☐ automatically provides an IP address to anyone.
- ☐ increases the risks associated with Wireless Encryption Protocol (WEP).

Explanation:

Explanation:

Dynamic Host Configuration Protocol (DHCP) automatically assigns IP addresses to anyone connected to the network. With DHCP disabled, static IP addresses must be used and represent less risk due to the potential for address contention between an unauthorized device and existing devices on the network. Choice B is incorrect because DHCP is suitable for small networks.

Choice C is incorrect because DHCP does not provide IP addresses when disabled. Choice D is incorrect because disabling of the DHCP makes it more difficult to exploit the well-known weaknesses in WEP.

Question 702

Which of the following would be of GREATEST concern to an IS auditor when auditing a small organization's purchasing department?

- ☐ The organization lacks a purchasing officer with experience in purchasing activities.
- ☐ Purchases can be approved after expenses have already been incurred.
- ☒ Some members of the department can request and approve payments for purchase requests.
- ☐ Purchasing procedures and processes have not been updated during the past two years.

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

Question 703

Nonrepudiation of the client for e-commerce transactions is accomplished through which of the following control mechanisms?

- ☐ Password security
- ☐ Internet protocol (IP) address verification
- ☒ Public key infrastructure (PKI)
- ☐ Secure Sockets Layer (SSL)

Question 704

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

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

Explanation:

Explanation:

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

Question 705

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

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

Question 706

The phases and deliverables of a system development life cycle (SDLC) project should be determined:

- ☒ during the initial planning stages of the project.
- ☐ after early planning has been completed, but before work has begun.
- ☐ throughout the work stages, based on risks and exposures.
- ☐ only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

Explanation:

Explanation:

It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

Question 707

Which of the following provides an IS auditor with the BEST evidence that an organization's information security program is aligned to business objectives?

- ☒ Balanced scorecard
- ☐ Risk assessment results
- ☐ Business impact analysis (BIA)
- ☐ Cost-benefit analysis

Question 708

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 709

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model depict data entities and how they relate?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☒ Entity relationship diagrams

Explanation:

Explanation:

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.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

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

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

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

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer – This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Context diagram – Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram – Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Context diagram – Outline the major processes of an organization and the external parties with which business interacts.

Activity or swim-lane diagram – De-construct business processes.

Reference:

CISA review manual 2014 Page number 188

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

Question 710

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 711

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

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

Question 712

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 713

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:

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

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

Question 714

When developing an escalation process for an incident response plan, the information security manager should PRIMARLY consider the:

- ☐ affected stakeholders
- ☐ availability of technical resources
- ☒ incident response team
- ☐ media coverage

Question 715

The MOST effective control for reducing the risk related to phishing is:

- ☐ centralized monitoring of systems.
- ☐ including signatures for phishing in antivirus software.
- ☐ publishing the policy on antiphishing on the intranet.
- ☒ security training for all users.

Explanation:

Explanation:

Phishing is a type of e-mail attack that attempts to convince a user that the originator is genuine, with the intention of obtaining information. Phishing is an example of a social engineering attack. Any social engineering type of attack can best Decontrolled through security and awareness training.

Question 716

The Federal Information Processing Standards (FIPS) are primarily for use by (Choose two.):

- ☒ all non-military government agencies
- ☒ US government contractors
- ☐ all military government agencies
- ☐ all private and public colleges in the US
- ☐ None of the choices.

Explanation:

Explanation:

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all nonmilitary government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community.

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

Question 717

When implementing a new risk assessment methodology, which of the following is the MOST important requirement?

- ☐ The methodology must be approved by the chief executive officer.
- ☐ Risk assessments must be reviewed annually.
- ☐ Risk assessments must be conducted by certified staff.
- ☒ The methodology used must be consistent across the organization.

Question 718

When evaluating the ability of a disaster recovery plan to enable the recovery of IT processing capabilities, it is MOST important for the IS auditor to verify the plan is:

- ☐ stored at an offsite location
- ☐ communicated to department heads
- ☒ regularly reviewed
- ☐ periodically tested

Question 719

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 720

In the absence of technical controls, what would be the BEST way to reduce unauthorized text messaging on company-supplied mobile devices?

- ☐ Update the corporate mobile usage policy to prohibit texting.
- ☐ Conduct a business impact analysis (BIA) and provide the report to management.
- ☐ Stop providing mobile devices until the organization is able to implement controls.
- ☒ Include the topic of prohibited texting in security awareness training.

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

Question 721

Which of the following is the BEST indication of an effective incident management process?

- ☐ Percentage of incidents where root cause has been identified
- ☒ Percentage of incidents closed without escalation
- ☐ Number of calls to the help desk
- ☐ Number of incidents reviewed by the IT management

Question 722

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 723

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

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

Question 724

Which of the following step of PDCA implement the plan, execute the process and make product?

- ☐ Plan
- ☒ Do
- ☐ Check
- ☐ Act

Explanation:

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:

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).

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

Reference:

CISA review manual 2014 page number 107

Question 725

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.

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

Question 726

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 727

Which of the following is an implementation risk within the process of decision support systems?

- ☐ Management control
- ☐ Semistructured dimensions
- ☒ inability to specify purpose and usage patterns
- ☐ Changes in decision processes

Explanation:

Explanation:

The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DDS.

Question 728

Which of the following software development methodology is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☒ Component based development

Explanation:

Explanation:

Component-based software engineering (CBSE) (also known as component-based development (CBD)) is a branch of software engineering that emphasizes the separation of concerns in respect of the wide-ranging functionality available throughout a given software system. It is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems. This practice aims to bring about an equally wide-ranging degree of benefits in both the short-term and the long-term for the software itself and for organizations that sponsor such software.

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

Software engineers[who?] regard components as part of the starting platform for service-orientation. Components play this role, for example, in web services, and more recently, in service-oriented architectures (SOA), whereby a component is converted by the web service into a service and subsequently inherits further characteristics beyond that of an ordinary component.

Components can produce or consume events and can be used for event-driven architectures (EDA).

Definition and characteristics of components

An individual software component is a software package, a web service, a web resource, or a module that encapsulates a set of related functions (or data).

All system processes are placed into separate components so that all of the data and functions inside each component are semantically related (just as with the contents of classes). Because of this principle, it is often said that components are modular and cohesive.

With regard to system-wide co-ordination, components communicate with each other via interfaces. When a component offers services to the rest of the system, it adopts a provided interface that specifies the services that other components can utilize, and how they can do so. This interface can be seen as a signature of the component - the client does not need to know about the inner workings of the component (implementation) in order to make use of it. This principle results in components referred to as encapsulated. The UML illustrations within this article represent provided interfaces by a lollipop-symbol attached to the outer edge of the component.

However, when a component needs to use another component in order to function, it adopts a used interface that specifies the services that it needs. In the UML illustrations in this article, used interfaces are represented by an open socket symbol attached to the outer edge of the component.

A simple example of several software components - pictured within a hypothetical holiday-reservation system represented in UML 2.0.

Another important attribute of components is that they are substitutable, so that a component can replace another (at design time or run-time), if the successor component meets the requirements of the initial component (expressed via the interfaces). Consequently, components can be replaced with either an updated version or an alternative without breaking the system in which the component operates.

As a general rule of thumb for engineers substituting components, component B can immediately replace component A, if component B provides at least what component A provided and uses no more than what component A used.

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

Software components often take the form of objects (not classes) or collections of objects (from object-oriented programming), in some binary or textual form, adhering to some interface description language (IDL) so that the component may exist autonomously from other components in a computer.

When a component is to be accessed or shared across execution contexts or network links, techniques such as serialization or marshalling are often employed to deliver the component to its destination.

Reusability is an important characteristic of a high-quality software component. Programmers should design and implement software components in such a way that many different programs can reuse them. Furthermore, component-based usability testing should be considered when software components directly interact with users.

It takes significant effort and awareness to write a software component that is effectively reusable. The component needs to be:

fully documented

thoroughly tested

robust - with comprehensive input-validity checking

able to pass back appropriate error messages or return codes

designed with an awareness that it will be put to unforeseen uses

The following were incorrect answers:

Agile Development - Agile software development is a group of software development methods based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams.

Software prototyping- Software prototyping, refers to the activity of creating prototypes of software applications, i.e., incomplete versions of the software program being developed. It is an activity that can occur in software development and is comparable to prototyping as known from other fields, such as mechanical engineering or manufacturing.

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

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.

Reference:

CISA review manual 2014 Page number 194

Question 729

Which of the following is the GREATEST risk of using a reciprocal site for disaster recovery?

- ☐ Inability to utilize the site when required
- ☒ Inability to test the recovery plans onsite
- ☐ Mismatched organizational security policies
- ☐ Equipment compatibility issues at the site

Question 730

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 731

Which of the following step of PDCA study the actual result and compares it against the expected result?

- ☐ Plan
- ☐ Do
- ☒ Check
- ☐ Act

Explanation:

Explanation:

Check - Study the actual results (measured and collected in "DO" above) and compare against the expected results (targets or goals from the "PLAN") to ascertain any differences. Look for deviation in implementation from the plan and also look for the appropriateness and completeness of the plan to enable the execution, i.e., "Do". Charting data can make this much easier to see trends over several

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

PDCA cycles and in order to convert the collected data into information. Information is what you need for the next step "ACT".

For your exam you should know the information below:

PDCA (plan–do–check–act or plan–do–check–adjust) is an iterative four-step management method used in business for the control and continuous improvement of processes and products. It is also known as the Deming circle/cycle/wheel, Stewart cycle, control circle/cycle, or plan–do–study–act (PDSA). Another version of this PDCA cycle is OPDCA. The added "O" stands for observation or as some versions say "Grasp the current condition."

The steps in each successive PDCA cycle are:

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".

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

ACT

Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product. When a pass through these four steps does not result in the need to improve, the scope to which PDCA is applied may be refined to plan and improve with more detail in the next iteration of the cycle, or attention needs to be placed in a different stage of the process.

The following answers are incorrect:

PLAN - Establish the objectives and processes necessary to deliver results in accordance with the expected output (the target or goals).

DO - Implement the plan, execute the process, make the product. Collect data for charting and analysis in the following "CHECK" and "ACT" steps.

ACT -Request corrective actions on significant differences between actual and planned results. Analyze the differences to determine their root causes. Determine where to apply changes that will include improvement of the process or product

Reference:

CISA review manual 2014 page number 107

Question 732

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:

Explanation:

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

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

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

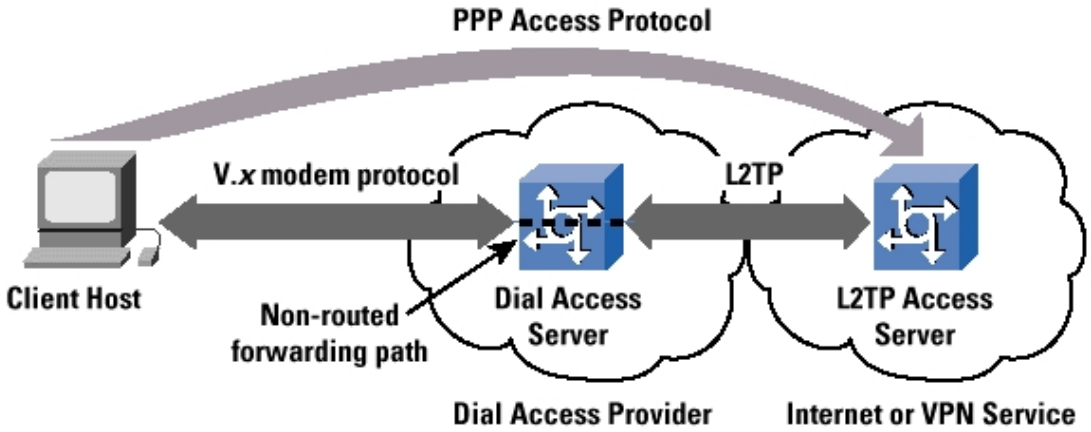
Point-to-point protocol

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

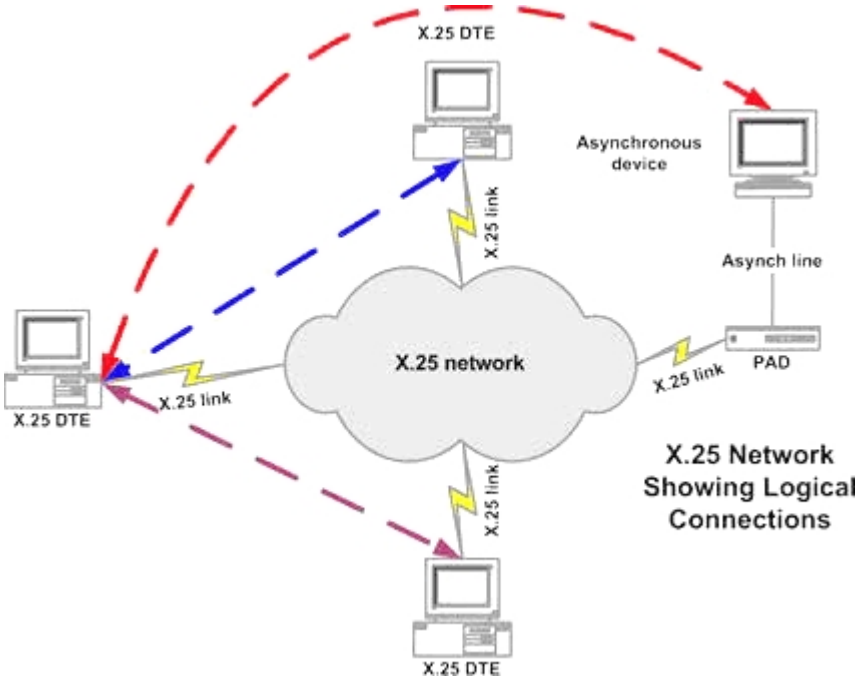
X.25 is an ITU-T standard protocol suite for packet switched wide area network (WAN) communication.

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

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

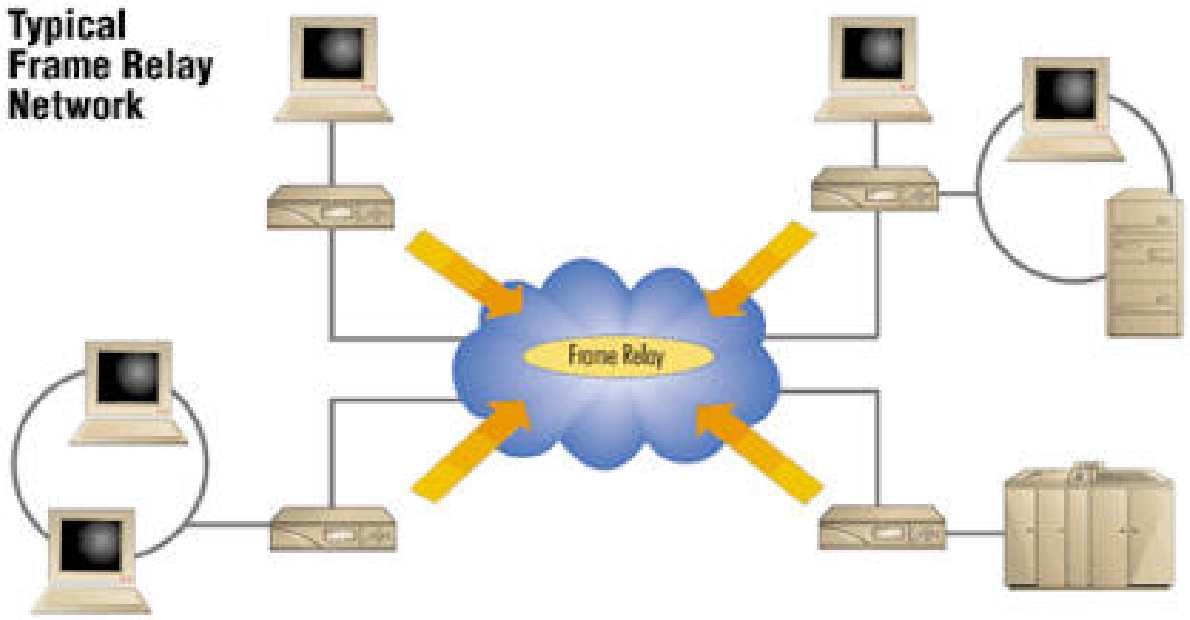
Two main types of equipment’s are used in Frame Relay

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.

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

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

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

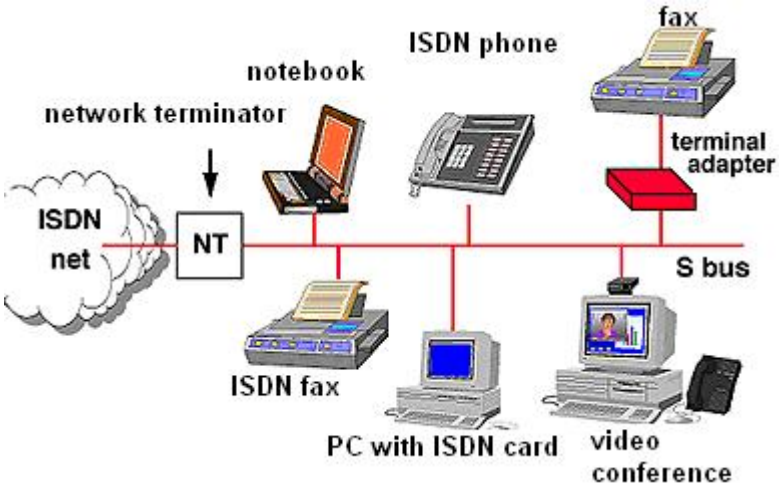
Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

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

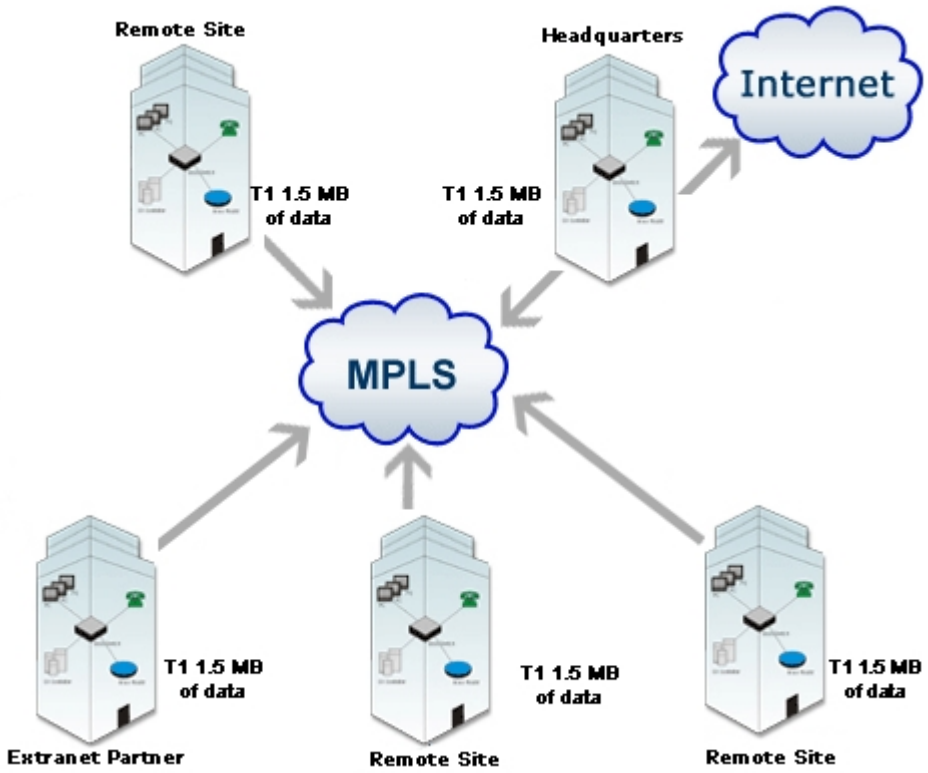
Asynchronous Transfer Mode

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.

Reference:

CISA review manual 2014 page number 266

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

Question 733

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 734

Which of the following is the MOST effective way to prevent unauthorized changes from being moved into production?

- ☐ Conduct periodic review of change tickets to ensure all change documentation is attached.
- ☐ Enforce segregation of duties between developers and migrators.
- ☒ Perform thorough testing of changes in the test environment.
- ☐ Require approval of changes by the appropriate business process owners.

Question 735

An IS auditor is performing a post-implementation review of a system deployed two years ago. Which of the following findings should be of MOST concern to the auditor?

- ☐ Maintenance costs were not included in the project lifecycle costs.
- ☒ Benefits as stated in the business case have not been realized.
- ☐ Workarounds due to remaining defects had to be used longer than anticipated.
- ☐ The system has undergone several change requests to further extend functionality.

Question 736

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.

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

Question 737

During a review of operations, it is noted that during a batch update, an error was detected and the database initiated a roll-back. An IT operator stopped the roll-back and re-initiated the update. What should the operator have done PRIOR to re-initiating the update?

- ☒ Determined the cause of the error
- ☐ Obtained approval before re-initiating the update
- ☐ Allowed the roll-back to complete
- ☐ Scheduled the roll-back for a later time

Question 738

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

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

Question 739

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:

Explanation:

Harming is a cyber attack intended to redirect a website's traffic to another, bogus site. Harming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Harming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

The term "phrasing" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both phrasing and phishing have been used to gain information for online identity theft. Phrasing has become of major concern to businesses hosting ecommerce and online banking 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.

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

For your exam you should know the information below:

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

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

Link manipulation

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

Website forgery

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

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

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

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.

Reference:

CISA review manual 2014 Page number 323

Official ISC2 guide to CISSP CBK 3rd Edition Page number326

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

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

Question 740

Which of the following protects against the impact of temporary and rapid decreases or increases in electricity?

- ☐ Redundant power supply
- ☐ Emergency power-off switch
- ☐ Stand-by generator
- ☒ Uninterruptible power supply (UPS)

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

Question 741

An IS auditor examining a biometric user authentication system establishes the existence of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Of the following, which is the BEST control against this risk?

- ☒ Kerberos
- ☐ Vitality detection
- ☐ Multimodal biometrics
- ☐ Before-image/after-image logging

Explanation:

Explanation:

Kerberos is a network authentication protocol for client-server applications that can be used to restrict access to the database to authorized users. Choices B and C are incorrect because vitality detection and multimodal biometrics are controls against spoofing and mimicry attacks. Before-image/after-image logging of database transactions is a detective control, as opposed to Kerberos, which is a preventative control.

Question 742

An organization has just completed their annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?

- ☒ Review and evaluate the business continuity plan for adequacy
- ☐ Perform a full simulation of the business continuity plan
- ☐ Train and educate employees regarding the business continuity plan
- ☐ Notify critical contacts in the business continuity plan

Explanation:

Explanation:

The business continuity plan should be reviewed every time a risk assessment is completed for the organization. Training of the employees and a simulation should be performed after the business continuity plan has been deemed adequate for the organization. There is no reason to notify the business continuity plan contacts at this time.

Question 743

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:

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

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:

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.

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

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer – Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer – This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer – This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer – This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer – Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

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

Warehouse Management Layer – The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

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 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.

Reference:

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

CISA review manual 2014 Page number 188

Question 744

The MOST important function of a business continuity plan is to:

- ☒ ensure that the critical business functions can be recovered
- ☐ provide procedures for evaluating tests of the business continuity plan
- ☐ provide a schedule of events that has to occur if there is a disaster
- ☐ ensure that all business functions are restored

Question 745

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 746

Which of the following control fixes a component or system after an incident has occurred?

- ☐ Deterrent
- ☐ Preventive
- ☒ Corrective
- ☐ Recovery

Explanation:

Explanation:

Corrective control fixes components or systems after an incident has occurred

For your exam you should know below information about different security controls

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

Recovery - Recovery controls are intended to bring the environment back to regular operations

Reference:

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 747

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 748

Which of the following actions should an organization's security policy require an employee to take upon finding a security breach?

- ☒ Report the incident to the manager immediately.
- ☐ Inform IS audit management immediately.
- ☐ Confirm the breach can be exploited.
- ☐ Devise appropriate countermeasures.

Question 749

Which of the following is the BEST indication of a successful information security culture?

- ☐ Penetration testing is done regularly and findings remediated.
- ☒ End users know how to identify and report incidents.
- ☐ Individuals are given access based on job functions.
- ☐ The budget allocated for information security is sufficient.

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

Question 750

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.

Question 751

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 752

Which of the following is widely accepted as one of the critical components in networking management?

- ☒ Configuration management
- ☐ Topological mappings
- ☐ Application of monitoring tools
- ☐ Proxy server troubleshooting

Explanation:

Explanation:

Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally, it also deals with the management of configuration and monitoring performance. Topological mappings provide outlines

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

of the components of the network and its connectivity. Application monitoring is not essential and proxy server troubleshooting is used for troubleshooting purposes.

Question 753

Which of the following is the MOST likely cause of a successful firewall penetration?

- ☐ Use of a Trojan to bypass the firewall
- ☐ Loophole in firewall vendor's code
- ☐ Virus infection
- ☒ Firewall misconfiguration by the administrator

Question 754

Which of the following refers to the act of creating and using an invented scenario to persuade a target to perform an action?

- ☒ Pretexting
- ☐ Backgrounding
- ☐ Check making
- ☐ Bounce checking
- ☐ None of the choices.

Explanation:

Explanation:

Pretexting is the act of creating and using an invented scenario to persuade a target to release information or perform an action and is usually done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information.

Question 755

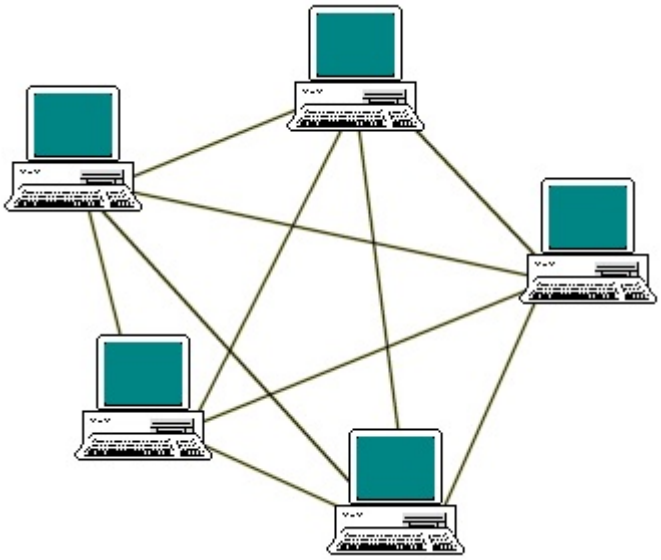
Which of the following BEST enables an audit department to improve the quality of work performed by its auditors?

- ☒ Implementing global quality standards
- ☐ Funding additional resources for audit work
- ☐ Using audit-related data analytics tools
- ☐ Implementing peer review of audit work

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

Question 756

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☒ Mesh

Explanation:

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.

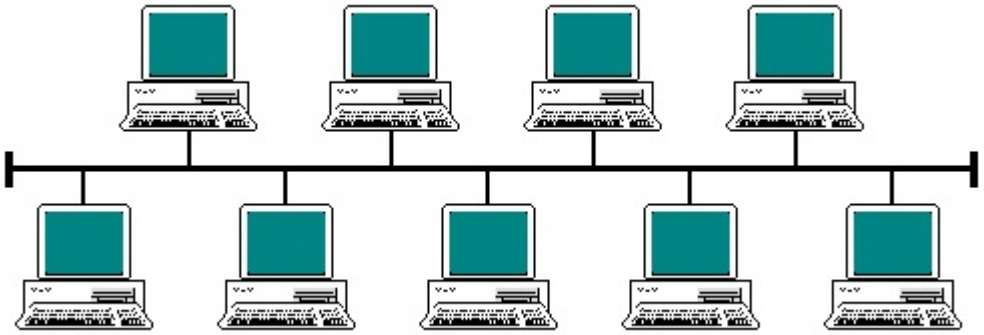
Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

Bus

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

In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.

Bus topology



Linear bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has exactly two endpoints (this is the 'bus', which is also commonly referred to as the backbone, or trunk) – all data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network simultaneously.

Distributed bus

The type of network topology in which all of the nodes of the network are connected to a common transmission medium which has more than two endpoints that are created by adding branches to the main section of the transmission medium – the physical distributed bus topology functions in exactly 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.

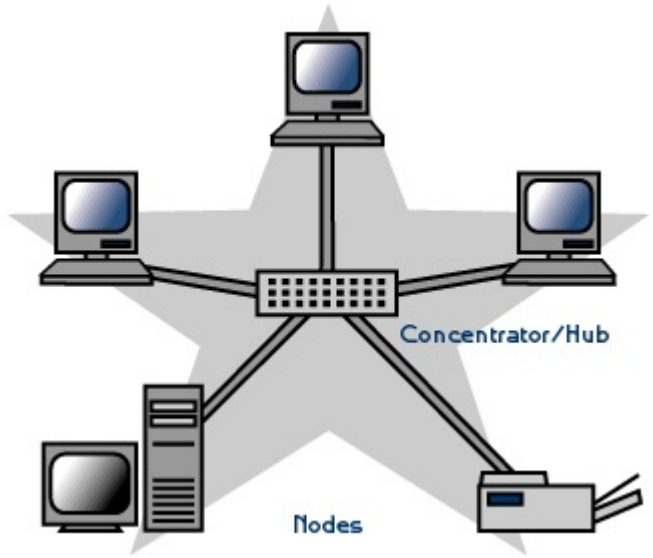
Licensed to Berend Post berend.post@it-university.nl

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



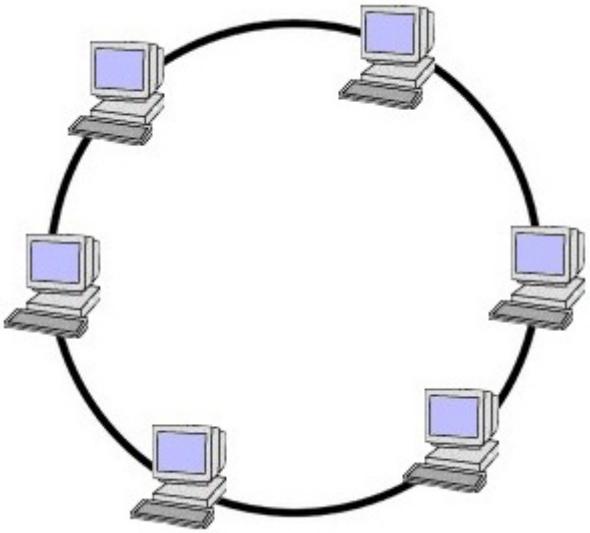
Ring

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

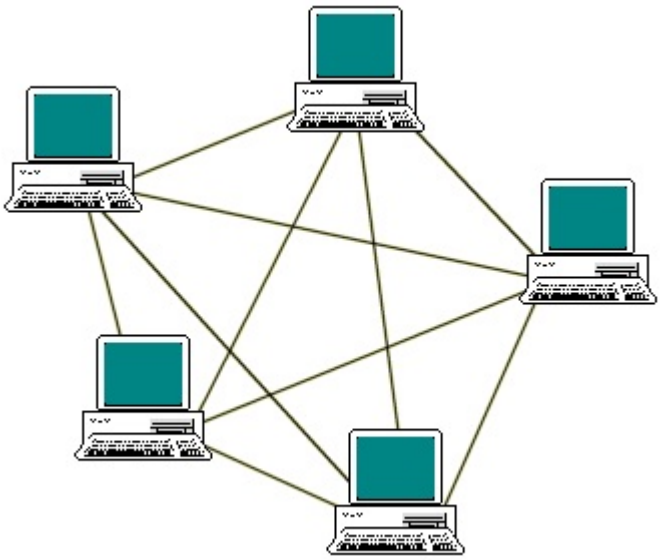


Mesh

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.

Reference:

CISA review manual 2014, Page number 262

Question 757

In a RACI model, which of the following roles must be assigned to only one individual?

- ☐ Responsible
- ☐ Informed
- ☐ Consulted
- ☒ Accountable

Question 758

_____ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance.

- ☐ Data custodians
- ☒ The board of directors and executive officers
- ☐ IT security administration
- ☐ Business unit managers

Explanation:

Explanation:

The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

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

Question 759

When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☒ The point at which controls are exercised as data flow through the system
- ☐ Only preventive and detective controls are relevant
- ☐ Corrective controls can only be regarded as compensating
- ☐ Classification allows an IS auditor to determine which controls are missing

Explanation:

Explanation:

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect, since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

Question 760

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 761

Who is ultimately responsible for providing requirement specifications to the software- development team?

- ☒ The project sponsor
- ☐ The project members
- ☐ The project leader
- ☐ The project steering committee

Explanation:

Explanation:

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

The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

Question 762

Which of the following is MOST important for an IS auditor to understand when planning an IS audit?

- ☒ Inherent risk of auditable areas
- ☐ Management focus on particular operations
- ☐ Number of high-risk auditable processes
- ☐ Availability of IS audit resources

Question 763

Performance monitoring tools report that servers are consistently above the recommended utilization capacity. Which of the following is the BEST recommendation of the IS auditor?

- ☒ Develop a capacity plan based on usage projections.
- ☐ Deploy load balancers.
- ☐ Monitor activity logs.
- ☐ Add servers until utilization is at target capacity.

Question 764

Which of the following should be an IS auditor's BEST recommendation to prevent installation of unlicensed software on employees' company-provided devices?

- ☒ Enforce audit logging of software installation activities.
- ☐ Restrict software installation authority to administrative users only.
- ☐ Implement software blacklisting.
- ☐ Remove unlicensed software from end-user devices.

Question 765

Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

- ☐ Attribute sampling
- ☒ Generalized audit software (GAS)
- ☐ Test data
- ☐ Integrated test facility (ITF)

Explanation:

Explanation:

Generalized audit software (GAS) would enable the auditor to review the entire invoice file to look for those items that meet the selection criteria. Attribute sampling would aid in identifying records

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

meeting specific conditions, but would not compare one record to another to identify duplicates. To detect duplicate invoice records, the IS auditor should check all of the items that meet the criteria and not just a sample of the items. Test data are used to verify program processing, but will not identify duplicate records. An integrated test facility (ITF) allows the IS auditor to test transactions through the production system, but would not compare records to identify duplicates.

Question 766

Which of the following would provide the highest degree of server access control?

- ☐ A mantrap-monitored entryway to the server room
- ☐ Host-based intrusion detection combined with CCTV
- ☐ Network-based intrusion detection
- ☒ A fingerprint scanner facilitating biometric access control

Explanation:

Explanation:

A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

Question 767

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 768

A company has located its computer center on a moderate earthquake fault. Which of the following is the MOST important consideration in establishing a contingency plan and an alternate processing site?

- ☒ The alternative site does not reside on the same fault no matter how far the distance apart.
- ☐ The contingency plan for high priority applications does not involve a shared cold site.
- ☐ The alternative site is a hot site with equipment ready to resume processing immediately.
- ☐ The contingency plan provides for backup tapes to be taken to the alternative site.

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

Question 769

A hot site should be implemented as a recovery strategy when the:

- ☒ disaster tolerance is low.
- ☐ recovery point objective (RPO) is high.
- ☐ recovery time objective (RTO) is high.
- ☐ disaster tolerance is high.

Explanation:

Explanation:

Disaster tolerance is the time gap during which the business can accept nonavailability of IT facilities. If this time gap is low, recovery strategies that can be implemented within a short period of time, such as a hot site, should be used. The RPO is the earliest point in time at which it is acceptable to recover the data. A high RPO means that the process can wait for a longer time. In such cases, other recovery alternatives, such as warm or cold sites, should be considered. A high RTO means that additional time would be available for the recovery strategy, thus making other recovery alternatives-such as warm or cold sites- viable alternatives.

Question 770

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

Question 771

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:

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

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 772

To develop a robust data security program, the FIRST course of action should be to:

- ☐ implement monitoring controls
- ☐ implement data loss prevention controls
- ☒ perform an inventory of assets
- ☐ interview IT senior management

Question 773

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- ☒ Response
- ☐ Correction
- ☐ Detection
- ☐ Monitoring

Explanation:

Explanation:

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

Question 774

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

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

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

Question 775

An organization is developing data classification standards and has asked internal audit for advice on aligning the standards with best practices. Internal audit would MOST likely recommend the standards should be:

- ☐ based on the results of an organization-wide risk assessment.
- ☐ based on the business requirements for confidentiality of the information.
- ☒ aligned with the organization's segregation of duties requirements.
- ☐ based on the business requirements for authentication of the information.

Question 776

An auditor is creating an audit program in which the objective is to establish the adequacy of personal data privacy controls in a payroll process. Which of the following would be MOST important to include?

- ☒ Approval of data changes
- ☐ Audit logging of administrative user activity
- ☐ Segregation of duties controls
- ☐ User access provisioning

Question 777

Which of the following is the PRIMARY objective of implementing privacy-related controls within an organization?

- ☐ To identify data at rest and data in transit for encryption
- ☐ To prevent confidential data loss
- ☒ To comply with legal and regulatory requirements
- ☐ To provide options to individuals regarding use of their data

Question 778

Which of the following is the BEST way to transmit documents classified as confidential over the Internet?

- ☐ Hashing the document contents and destroying the hash value
- ☐ Sending documents as multiple packets over different network routes
- ☐ Converting documents to proprietary format before transmission
- ☒ Using a virtual private network (VPN)

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

Question 779

The development of an IS security policy is ultimately the responsibility of the:

- ☐ IS department.
- ☐ security committee.
- ☐ security administrator.
- ☒ board of directors.

Explanation:

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

Question 780

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.

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

Question 781

To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

- ☐ online terminals are placed in restricted areas.
- ☐ online terminals are equipped with key locks.
- ☐ ID cards are required to gain access to online terminals.
- ☒ online access is terminated after a specified number of unsuccessful attempts.

Explanation:

Explanation:

The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through the guessing of IDs and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

Question 782

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

- ☒ Consider feasibility of a separate user acceptance environment
- ☐ Schedule user testing to occur at a given time each day
- ☐ implement a source code version control tool
- ☐ Only retest high priority defects

Explanation:

Explanation:

A separate environment or environments is normally necessary for testing to be efficient and effective, and to ensure the integrity of production code, it is important that the development and testing code base be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

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

Question 783

During a follow-up audit for a finding related to change management, an IS auditor notes that one of the changes sampled was an emergency change, which follows a different process. Which of the following is the auditor's BEST course of action?

- ☒ Mark the sample as not applicable in the workpaper and move or to testing the next sample.
- ☐ Select a replacement change for testing.
- ☐ Obtain evidence that the change was approved.
- ☐ Note the sample as a deviation and leave the finding open in the audit tracking log.

Question 784

The MOST effective biometric control system is the one:

- ☐ which has the highest equal-error rate (EER).
- ☒ which has the lowest EER.
- ☐ for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- ☐ for which the FRR is equal to the failure-to-enroll rate (FER).

Explanation:

Explanation:

The equal-error rate (EER) of a biometric system denotes the percent at which the false- acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

Question 785

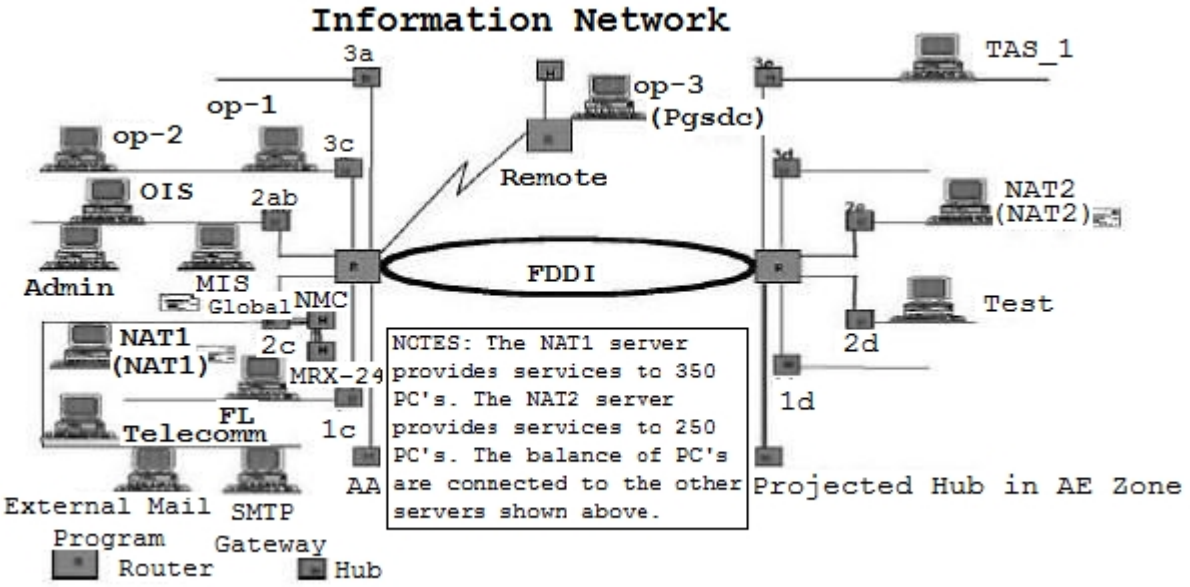
Which of the following is a detective control that can be used to uncover unauthorized access to information systems?

- ☐ Requiring long and complex passwords for system access
- ☒ Implementing a security information and event management (SIEM) system
- ☐ Requiring internal audit to perform periodic reviews of system access logs
- ☐ Protecting access to the data center with multifactor authentication

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

Question 786

For locations 3a, 1d and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?



- ☐ Intelligent hub
- ☐ Physical security over the hubs
- ☒ Physical security and an intelligent hub
- ☐ No controls are necessary since this is not a weakness

Explanation:

Explanation:

Open hubs represent a significant control weakness because of the potential to access a network connection easily. An intelligent hub would allow the deactivation of a single port while leaving the remaining ports active. Additionally, physical security would also provide reasonable protection over hubs with active ports.

Question 787

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- ☒ address audit objectives.
- ☐ collect sufficient evidence.
- ☐ specify appropriate tests.
- ☐ minimize audit resources.

Explanation:

Explanation:

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning.

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

The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

Question 788

Which of the following BEST supports the prioritization of new IT projects?

- ☐ Internal control self-assessment (CSA)
- ☐ Information systems audit
- ☒ Investment portfolio analysis
- ☐ Business risk assessment

Explanation:

Explanation:

It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal control self-assessment (CSA) may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects.

Business risk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

Question 789

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 790

An IS auditor is reviewing IT policies and found that most policies have not been reviewed in over 3 years. The MOST significant risk is that the policies do not reflect:

- ☒ current legal requirements.
- ☐ the vision of the CEO.
- ☐ the mission of the organization.
- ☐ current industry best practices.

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

Question 791

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- ☐ User acceptance testing (UAT) occur for all reports before release into production
- ☒ Organizational data governance practices be put in place
- ☐ Standard software tools be used for report development
- ☐ Management sign-off on requirements for new reports

Explanation:

Explanation:

This choice directly addresses the problem. An organization wide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

Question 792

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 793

An IS auditor finds that client requests were processed multiple times when received from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

- ☐ increase the frequency for data replication between the different department systems to ensure timely updates.
- ☐ Centralize all request processing in one department to avoid parallel processing of the same request.
- ☒ Change the application architecture so that common data is held in just one shared database for all departments.
- ☐ implement reconciliation controls to detect duplicates before orders are processed in the systems.

Explanation:

Explanation:

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

Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannot be eliminated completely because parallel data entry is still possible. Business requirements will most likely dictate where data processing activities are performed. Changing the business structure to solve an IT problem is not practical or politically feasible. Detective controls do not solve the problem of duplicate processing, and would require that an additional process be implemented to handle the discovered duplicates.

Question 794

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:

Explanation:

The following answers are incorrect:

All of the other choices are facilitated by a BCP:

the continuation of critical business functions

the rapid recovery of mission-critical business operations

the reduction of the impact of a disaster

Question 795

For which of the following applications would rapid recovery be MOST crucial?

- ☒ Point-of-sale system
- ☐ Corporate planning
- ☐ Regulatory reporting
- ☐ Departmental chargeback

Explanation:

Explanation:

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

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

Question 796

Which of the following is a network diagnostic tool that monitors and records network information?

- ☐ Online monitor
- ☐ Downtime report
- ☐ Help desk report
- ☒ Protocol analyzer

Explanation:

Explanation:

Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors (choice A) measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports (choice B) track the availability of telecommunication lines and circuits. Help desk reports (choice C) are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.

Question 797

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 798

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 799

Which of the following is MOST important for an IS auditor to verify when reviewing an organization's information security practices following the adoption of a bring your own device (BYOD) program?

- ☐ Only applications approved by information security may be installed on devices.
- ☐ The expected benefits of adopting the BYOD program have been realized.
- ☒ Security policies have been updated to include BYOD.
- ☐ Remote wipe is enabled for devices allowed by BYOD.

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

Question 800

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 801

What can be used to gather evidence of network attacks?

- ☐ Access control lists (ACL)
- ☒ Intrusion-detection systems (IDS)
- ☐ Syslog reporting
- ☐ Antivirus programs

Explanation:

Explanation:

Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

Question 802

Which of the following data would be used when performing a business impact analysis (BIA)?

- ☒ Projected impact of current business on future business
- ☐ Cost of regulatory compliance
- ☐ Cost benefit analysis of running the current business
- ☐ Expected costs for recovering the business.

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

Question 803

What supports data transmission through split cable facilities or duplicate cable facilities?

- ☒ Diverse routing
- ☐ Dual routing
- ☐ Alternate routing
- ☐ Redundant routing

Explanation:

Explanation:

Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

Question 804

What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

- ☐ Contrived data
- ☐ Independently created data
- ☐ Live data
- ☒ Data from previous tests

Explanation:

Explanation:

Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

Question 805

There is a concern that a salesperson may download an organization's full customer list from the Software as a Service (SaaS) when leaving to work for a competitor. Which of the following would BEST help to identify this type of incident?

- ☒ Monitor applications logs
- ☐ Disable remote access to the application
- ☐ Implement a web application firewall
- ☐ Implement an intrusion detection system (IDS)

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

Question 806

An IS auditor conducts a review of a third-party vendor's reporting of key performance indicators (KPIs). Which of the following findings should be of MOST concern to the auditor?

- ☐ Some KPIs are not documented.
- ☐ KPIs have never been updated.
- ☐ KPIs data is not being analyzed.
- ☒ KPIs are not clearly defined.

Question 807

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- ☒ registration authority (RA).
- ☐ issuing certification authority (CA).
- ☐ subject CA.
- ☐ policy management authority.

Explanation:

Explanation:

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

Question 808

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.

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

Question 809

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 810

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.

Question 811

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.

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

Question 812

Management has agreed to perform multiple remediation actions in response to an audit issue, including the implementation of a new control. Which of the following is the BEST time for an IS auditor to perform an audit follow-up of this issue?

- ☒ After management has completed the required actions
- ☐ When audit resources are available
- ☐ When management resources are available
- ☐ After the new control has been in place for one year

Question 813

An IS auditor is evaluating the risk associated with moving from one database management system to another. Which of the following would be MOST helpful to ensure the integrity of the system throughout the change?

- ☐ Preserving the same data structure
- ☐ Preserving the same data classifications
- ☐ Preserving the same data interfaces
- ☒ Preserving the same data inputs

Question 814

What is the BEST way to control updates to the vendor master file in an accounts payable system?

- ☒ Using prenumbered and authorized request forms
- ☐ Having only one person updating the master file
- ☐ Periodically reviewing the entire vendor master file
- ☐ Comparing updates against authorization

Question 815

Both statistical and nonstatistical sampling techniques:

- ☒ permit the auditor to quantify the probability of error.
- ☐ permit the auditor to quantify and fix the level of risk.
- ☐ require judgment when defining population characteristics.
- ☐ provide each item an equal opportunity of being selected.

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

Question 816

The PRIMARY objective of a logical access control review is to:

- ☐ review access controls provided through software.
- ☒ ensure access is granted per the organization's authorities.
- ☐ walk through and assess the access provided in the IT environment.
- ☐ provide assurance that computer hardware is adequately protected against abuse.

Explanation:

Explanation:

The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

Question 817

What is often assured through table link verification and reference checks?

- ☒ Database integrity
- ☐ Database synchronization
- ☐ Database normalcy
- ☐ Database accuracy

Explanation:

Explanation:

Database integrity is most often ensured through table link verification and reference checks.

Question 818

Which of the following is the MOST important factor when an organization is developing information security policies and procedures?

- ☐ Cross-references between policies and procedures
- ☐ Inclusion of mission and objectives
- ☒ Compliance with relevant regulations
- ☐ Consultation with management

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

Question 819

Which of the following is the BEST point in time to conduct a post-implementation review (PIR)?

- ☒ After a full processing cycle
- ☐ Immediately after deployment
- ☐ To coincide with annual PIR cycle
- ☐ Six weeks after deployment

Question 820

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 821

An organization has recently incorporated robotic process automation. Which of the following would be of GREATEST concern to an IS auditor?

- ☐ Controls have not been tested
- ☐ A governance structure has not been implemented
- ☒ A risk assessment has not been conducted
- ☐ The adoption rate for the new technology has been low

Question 822

The performance of an order-processing system can be measured MOST reliably by monitoring:

- ☐ input/request queue length.
- ☒ turnaround time of completed transactions.
- ☐ application and database servers' CPU load.
- ☐ heartbeats between server systems.

Question 823

Which of the following could provide an organization with the fastest resumption of processing following a disk failure?

- ☐ Server load balancing
- ☒ Mirroring
- ☐ Open database connectivity (ODBC) of the backup server
- ☐ Replication

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

Question 824

Which of the following should be the MOST important criterion in evaluating a backup solution for sensitive data that must be retained for a long period of time due to regulatory requirements?

- ☐ Full backup window
- ☐ Media costs
- ☐ Restore window
- ☒ Media reliability

Explanation:

Explanation:

To comply with regulatory requirements, the media should be reliable enough to ensure an organization's ability to recovery the data should they be required for any reason. Media price is a consideration, but should not be more important than the ability to provide the required reliability. Choices A and C are less critical than reliability.

Question 825

Reverse proxy technology for web servers should be deployed if:

- ☒ http servers' addresses must be hidden.
- ☐ accelerated access to all published pages is required.
- ☐ caching is needed for fault tolerance.
- ☐ bandwidth to the user is limited.

Explanation:

Explanation:

Reverse proxies are primarily designed to hide physical and logical internal structures from outside access. Complete URLs or URIs can be partially or completely redirected without disclosing which internal or DMZ server is providing the requested data. This technology might be used if a trade-off between security, performance and costs has to be achieved. Proxy servers cache some data but normally cannot cache all pages to be published because this depends on the kind of information the web servers provide. The ability to accelerate access depends on the speed of the back-end servers, i.e., those that are cached. Thus, without making further assumptions, a gain in speed cannot be assured, but visualization and hiding of internal structures can. If speed is an issue, a scale- out approach (avoiding adding additional delays by passing firewalls, involving more servers, etc.) would be a better solution. Due to the limited caching option, reverse proxies are not suitable for enhancing fault tolerance. User requests that are handled by reverse proxy servers are using exactly the same bandwidth as direct requests to the hosts providing the data.

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

Question 826

Implementing a strong password policy is part of an organization's information security strategy for the year. A business unit believes the strategy may adversely affect a client's adoption of a recently developed mobile application and has decided not to implement the policy. Which of the following would be the information security manager's BEST course of action?

- ☒ Analyze the risk and impact of not implementing the policy
- ☐ Develop and implement a password policy for the mobile application
- ☐ Escalate non-implementation of the policy to senior management
- ☐ Benchmark with similar mobile applications to identify gaps

Question 827

An IS auditor is asked to review a large organization's change management process. Which of the following practices presents the GREATEST risk?

- ☐ Emergency code changes are promoted without user acceptance testing.
- ☐ A system administrator performs code migration on planned downtime.
- ☒ Change management tickets do not contain specific documentation.
- ☐ Transaction data changes can be made by a senior developer.

Question 828

Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

- ☐ Server antivirus software
- ☒ Virus walls
- ☐ Workstation antivirus software
- ☐ Virus signature updating

Explanation:

Explanation:

An important means of controlling the spread of viruses is to detect the virus at the point of entry, before it has an opportunity to cause damage. In an interconnected corporate network, virus scanning software, used as an integral part of firewall technologies, is referred to as a virus wall. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. The presence of virus walls does not preclude the necessity for installing virus detection software on servers and workstations within the network, but network- level protection is most effective the earlier the virus is detected. Virus signature updating is a must in all circumstances, networked or not.

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

Question 829

Which of the following is a substantive test procedure?

- ☒ Using audit software to verify the total of an accounts receivable file
- ☐ Observing that user IDs and passwords are required to sign on to the online system
- ☐ Test of invoice calculation process
- ☐ Verifying that appropriate approvals are documented in a sample of program changes

Question 830

Which of the following threats is MOST effectively controlled by a firewall?

- ☒ Network congestion
- ☐ Denial of service (DoS) attack
- ☐ Network sniffing
- ☐ Password cracking

Question 831

To ensure the integrity of a recovered database, which of the following would be MOST useful?

- ☒ Before-and-after transaction images
- ☐ Database defragmentation tools
- ☐ A copy of the data dictionary
- ☐ Application transaction logs

Question 832

Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

- ☐ Processing power
- ☐ Volume of data
- ☒ Key distribution
- ☐ Complexity of the algorithm

Explanation:

Explanation:

Symmetric key encryption requires that the keys be distributed. The larger the user group, the more challenging the key distribution. Symmetric key cryptosystems are generally less complicated and, therefore, use less processing power than asymmetric techniques, thus making it ideal for encrypting a large volume of data. The major disadvantage is the need to get the keys into the hands of those with whom you want to exchange data, particularly in e-commerce environments, where customers are unknown, untrusted entities

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

Question 833

Which of the following is the BEST way to evaluate the effectiveness of access controls to an internal network?

- ☒ Perform a system penetration test
- ☐ Test compliance with operating procedures
- ☐ Review access rights
- ☐ Review router configuration tables

Question 834

An organization with high availability resource requirements is selecting a provider for cloud computing. Which of the following would cause the GREATEST concern to an IS auditor? The provider:

- ☐ is not internationally certified for high availability.
- ☐ does not store backup media offsite.
- ☒ deploys patches automatically without testing.
- ☐ hosts systems for the organization's competitor.

Question 835

Regarding digital signature implementation, which of the following answers is correct?

- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
- ☒ A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Explanation:

Explanation:

A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

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

Question 836

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

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

Question 837

A digital signature contains a message digest to:

- ☒ show if the message has been altered after transmission.
- ☐ define the encryption algorithm.
- ☐ confirm the identity of the originator.
- ☐ enable message transmission in a digital format.

Explanation:

Explanation:

The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. It does not define the algorithm or enable the transmission in digital format and has no effect on the identity of the user; it is there to ensure integrity rather than identity.

Question 838

Which of the following BEST helps to ensure data integrity across system interfaces?

- ☐ Environment segregation
- ☐ System backups
- ☒ Reconciliations
- ☐ Access controls

Question 839

Which of the following would an IS auditor consider to be the MOST significant risk associated with a project to reengineer a business process?

- ☐ The negative impact of change may not be documented.
- ☐ The project manager is inexperienced in information systems.
- ☒ Existing controls may be weakened or removed.
- ☐ Existing baseline processes may not be reported to management.

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

Question 840

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 841

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☒ MTD

Explanation:

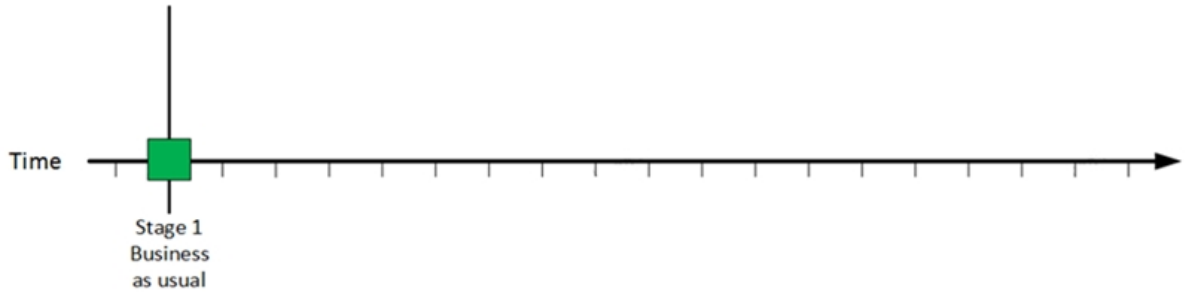
Explanation:

The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

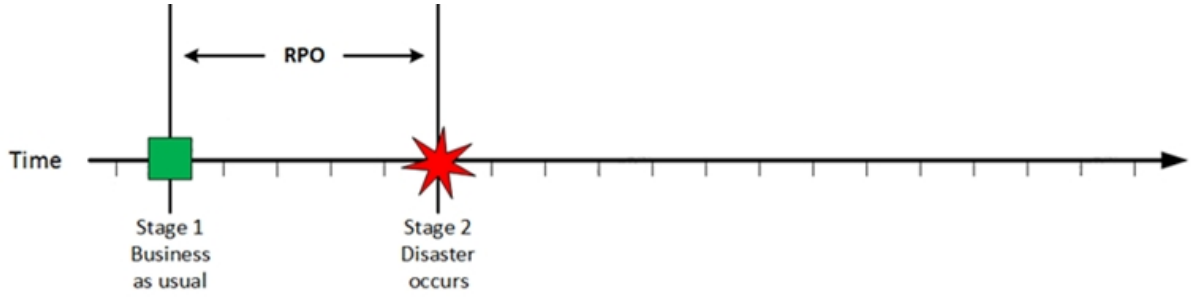


At this stage all systems are running production and working correctly.

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

Stage 2: Disaster occurs

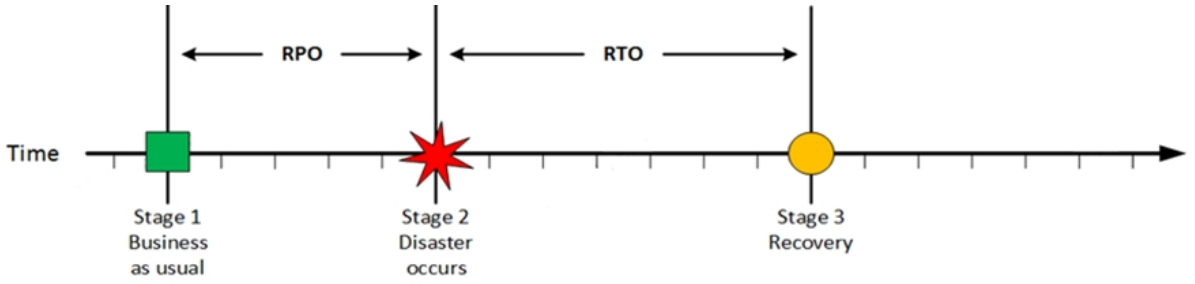
Disaster Occurs



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

Recovery

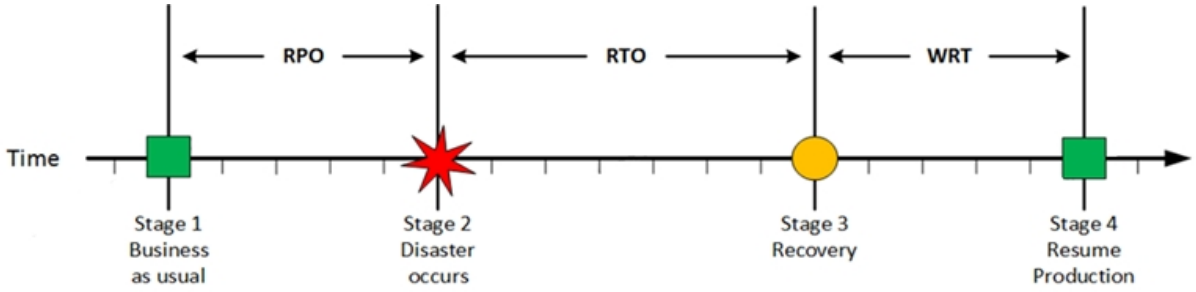


At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most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

Stage 4: Resume Production

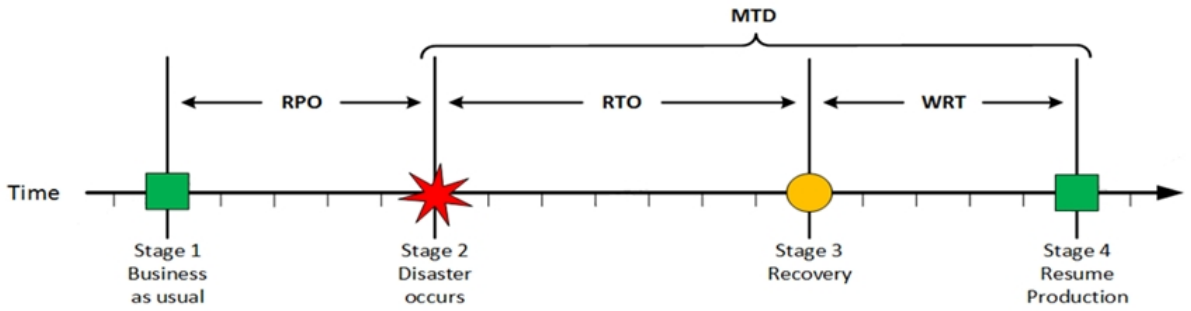
Resume Production

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



At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up

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

or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

Reference:

CISA review manual 2014 page number 284

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

Question 842

Which of the following is the MOST important factor when determining the frequency of information security risk reassessment?

- ☐ Audit findings
- ☐ Risk priority
- ☐ Mitigating controls
- ☒ Risk metrics

Question 843

An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:

- ☐ check to ensure that the type of transaction is valid for the card type.
- ☒ verify the format of the number entered then locate it on the database.
- ☐ ensure that the transaction entered is within the cardholder's credit limit.
- ☐ confirm that the card is not shown as lost or stolen on the master file.

Explanation:

Explanation:

The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in

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

place. Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

Question 844

Which of the following BEST helps to ensure that all relevant data within an organization is added to a data warehouse during deployment?

- ☒ Data migration
- ☐ Architecture review
- ☐ Project planning
- ☐ Data mining

Question 845

Which of the following statement INCORRECTLY describes circuit switching technique?

- ☒ Packet uses many different dynamic paths to get the same destination
- ☐ Connection oriented virtual links
- ☐ Fixed delays
- ☐ Traffic travels in a predictable and constant manner

Explanation:

Explanation:

The word INCORRECTLY is the keyword used in the question. You need to find out a statement which is not valid about circuit switching.

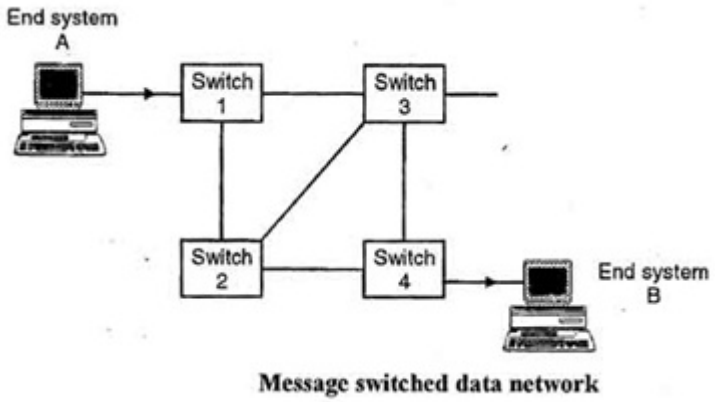
For your exam you should know below information about WAN message transmission technique:

Message Switching

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

Message Switching

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

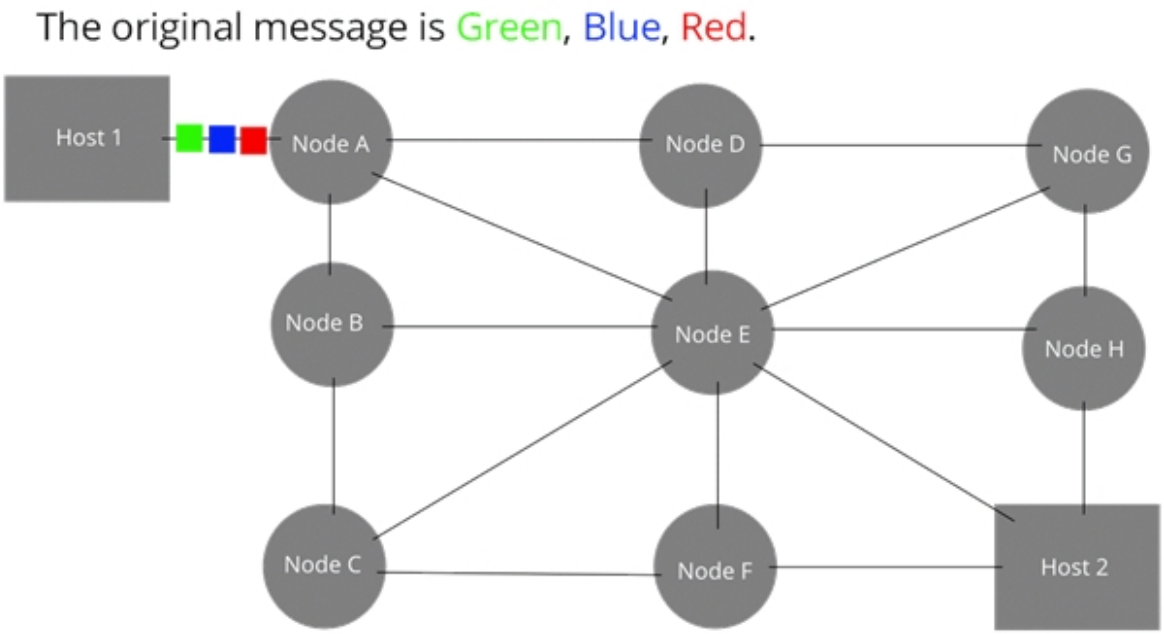


Message switched data network

Packet Switching

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

Packet Switching



Circuit Switching

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

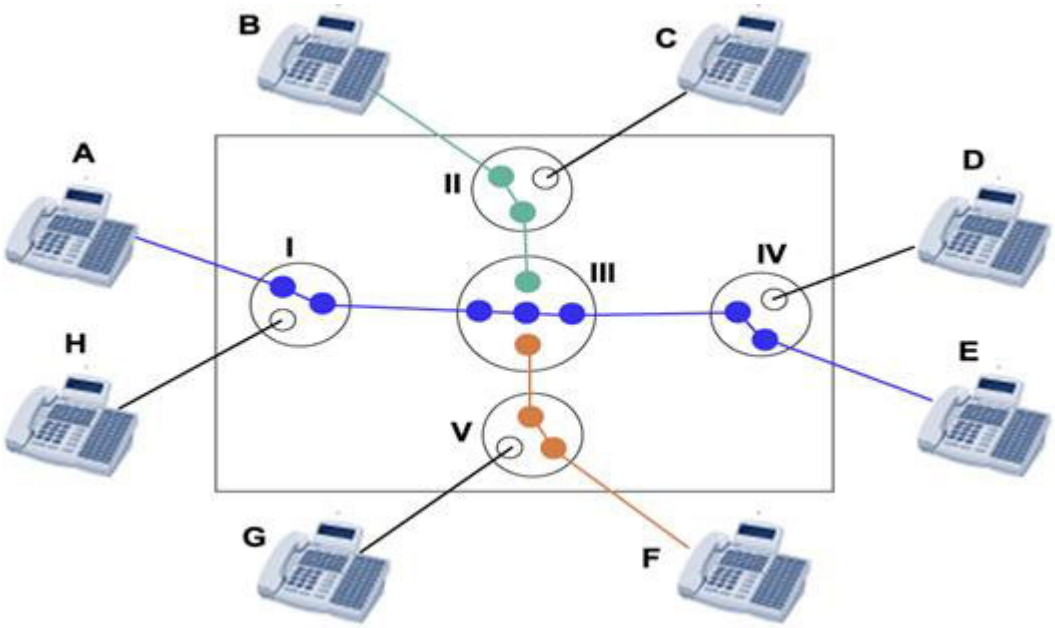
Licensed to Berend Post berend.post@it-university.nl

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

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

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

Circuit Switching



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

Difference between Circuit and packet switching

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

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

Virtual circuit

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

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

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

varying packet queue lengths in the network nodes,

varying bit rate generated by the application,

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

The following were incorrect answers:

The other options presented correctly describes about circuit switching.

Reference:

CISA review manual 2014 Page number 265

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

Question 846

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 847

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

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

Question 848

An IS auditor notes that a number of application plug-ins currently in use are no longer supported. Which of the following is the auditor's BEST recommendation to management?

- ☐ Implement role-based access controls.
- ☒ Conduct a vulnerability assessment to determine exposure.
- ☐ Review content backup and archiving procedures.
- ☐ Review on-boarding and off-boarding processes.

Question 849

Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following?

- ☐ Unsynchronized transactions
- ☒ Unauthorized transactions
- ☐ Inaccurate transactions
- ☐ Incomplete transactions

Explanation:

Explanation:

Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

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

Question 850

While executing follow-up activities, an IS auditor is concerned that management has implemented corrective actions that are different from those originally discussed and agreed with the audit function. In order to resolve the situation, the IS auditor's BEST course of action would be to:

- ☒ determine whether the alternative controls sufficiently mitigate the risk and record the results.
- ☐ reject the alternative controls and re-prioritize the original issue as high risk.
- ☐ postpone follow-up activities and escalate the alternative controls to senior audit management.
- ☐ schedule another audit due to the implementation of alternative controls.

Question 851

A recent audit has identified that security controls required by the organization's policies have not been implemented for a particular application. What should the information security manager do NEXT to address this issue?

- ☐ Deny access to the application until the issue is resolved.
- ☐ Discuss the issue with data custodians to determine the reason for the exception.
- ☐ Report the issue to senior management and request funding to fix the issue.
- ☒ Discuss the issue with data owners to determine the reason for the exception.

Question 852

Which of the following provides the BEST evidence that network filters are functioning?

- ☐ Reviewing network configuration rules
- ☒ Reviewing network filtering policy
- ☐ Performing network port scans
- ☐ Analyzing network performance

Question 853

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- ☐ Report the risks to the CIO and CEO immediately
- ☐ Examine e-business application in development
- ☒ Identify threats and likelihood of occurrence
- ☐ Check the budget available for risk management

Explanation:

Explanation:

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

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

Question 854

During an audit, it is discovered that several suppliers with standing orders have been deleted from the supplier master file. Which of the following controls would have BEST prevented such an occurrence?

- ☒ Logical relationship check
- ☐ Existence check
- ☐ Table look-ups
- ☐ Referential integrity

Question 855

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 856

Which of the following term related to network performance refers to the delay that packet may experience on their way to reach the destination from the source?

- ☐ Bandwidth
- ☐ Throughput
- ☒ Latency
- ☐ Jitter

Explanation:

Explanation:

Latency the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses.

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

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

The latency assumption seems to be that data should be transmitted instantly between one point and another (that is, with no delay at all). The contributors to network latency include:

Propagation: This is simply the time it takes for a packet to travel between one place and another at the speed of light.

Transmission: The medium itself (whether optical fiber, wireless, or some other) introduces some delay. The size of the packet introduces delay in a round trip since a larger packet will take longer to receive and return than a short one.

Router and other processing: Each gateway node takes time to examine and possibly change the header in a packet (for example, changing the hop count in the time-to-live field).

Other computer and storage delays: Within networks at each end of the journey, a packet may be subject to storage and hard disk access delays at intermediate devices such as switches and bridges. (In backbone statistics, however, this kind of latency is probably not considered.)

For your exam you should know below information about Network performance:

Network performance refers to measurement of service quality of a telecommunications product as seen by the customer.

The following list gives examples of network performance measures for a circuit-switched network and one type of packet-switched network (ATM):

Circuit-switched networks: In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads. Other types of performance measures can include noise, echo and so on.

ATM: In an Asynchronous Transfer Mode (ATM) network, performance can be measured by line rate, quality of service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.

There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyze how the network will perform in each state, ensuring that the network will be optimally designed.

The following measures are often considered important:

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

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Latency - Latency is the delay between the sender and the receiver decoding it, this is mainly a function of the signals travel time, and processing time at any nodes the information traverses

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Error Rate - Error rate is the number of corrupted bits expressed as a percentage or fraction of the total sen

The following answers are incorrect:

Bandwidth - Bandwidth is commonly measured in bits/second is the maximum rate that information can be transferred

Throughput - Throughput is the actual rate that information is transferred

Jitter - Jitter is the variation in the time of arrival at the receiver of the information

Reference:

CISA review manual 2014 page number 275

Question 857

Which of the following activities is MOST important to consider when conducting IS audit planning?

- ☐ Results from previous audits are reviewed.
- ☐ Audit scheduling is based on skill set of audit team.
- ☒ Resources are allocated to areas of high risk.
- ☐ The audit committee agrees on risk rankings.

Question 858

Which of the following is MOST important in determining a project's feasibility?

- ☐ The organization's main competitor has initiated a similar project.
- ☐ The IT steering committee endorses the project.
- ☐ A project management methodology is established.
- ☒ The project's value is established in an approved business case.

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

Question 859

Which of the following is the GREATEST risk associated with the lack of an effective data privacy program?

- ☐ Failure to prevent fraudulent transactions
- ☐ Inability to manage access to private or sensitive data
- ☐ Inability to obtain customer confidence
- ☒ Failure to comply with data-related regulations

Question 860

When determining which IS audits to conduct during the upcoming year, internal audit has received a request from management for multiple audits of the contract division due to fraud findings during the prior year. Which of the following is the BEST basis for selecting the audits to be performed?

- ☐ Select audits based on an organizational risk assessment.
- ☒ Select audits based on collusion risk.
- ☐ Select audits based on the skill sets of the IS auditors.
- ☐ Select audits based on management's suggestion.

Question 861

Which of the following malware technical fool's malware by appending section of themselves to files – somewhat in the same way that file malware appends themselves?

- ☐ Scanners
- ☐ Active Monitors
- ☒ Immunizer
- ☐ Behavior blocker

Explanation:

Explanation:

Immunizers defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

For your exam you should know below mentioned different kinds of malware Controls

A. Scanners – Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

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

1. Malware mask or Signatures – Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner – Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present)

Scanner examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers – Defend against malware by appending sections of themselves to files – sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker – Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker – Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however, they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

E. Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

The following were incorrect answers:

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

Scanners – Look for sequences of bit called signature that are typical malware programs.

Active Monitors – Active monitors interpret DOS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they can not distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

Behavior Blocker – Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

Reference:

CISA review manual 2014 Page number 354 and 355

Question 862

When replacing a critical software application, which of the following provides for the LOWEST risk of interruption to business processes?

- ☒ Parallel implementation
- ☐ Pilot implementation
- ☐ Incremental implementation
- ☐ Big-bang implementation

Question 863

Which of the following is the MOST critical step in planning an audit?

- ☐ Implementing a prescribed auditing framework such as COBIT
- ☐ Identifying current controls
- ☒ Identifying high-risk audit targets
- ☐ Testing controls

Explanation:

Explanation:

In planning an audit, the most critical step is identifying the areas of high risk.

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

Question 864

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

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

Question 865

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 866

Which of the following transmission media is MOST difficult to tap?

- ☐ Copper cable
- ☒ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Radio System

Explanation:

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

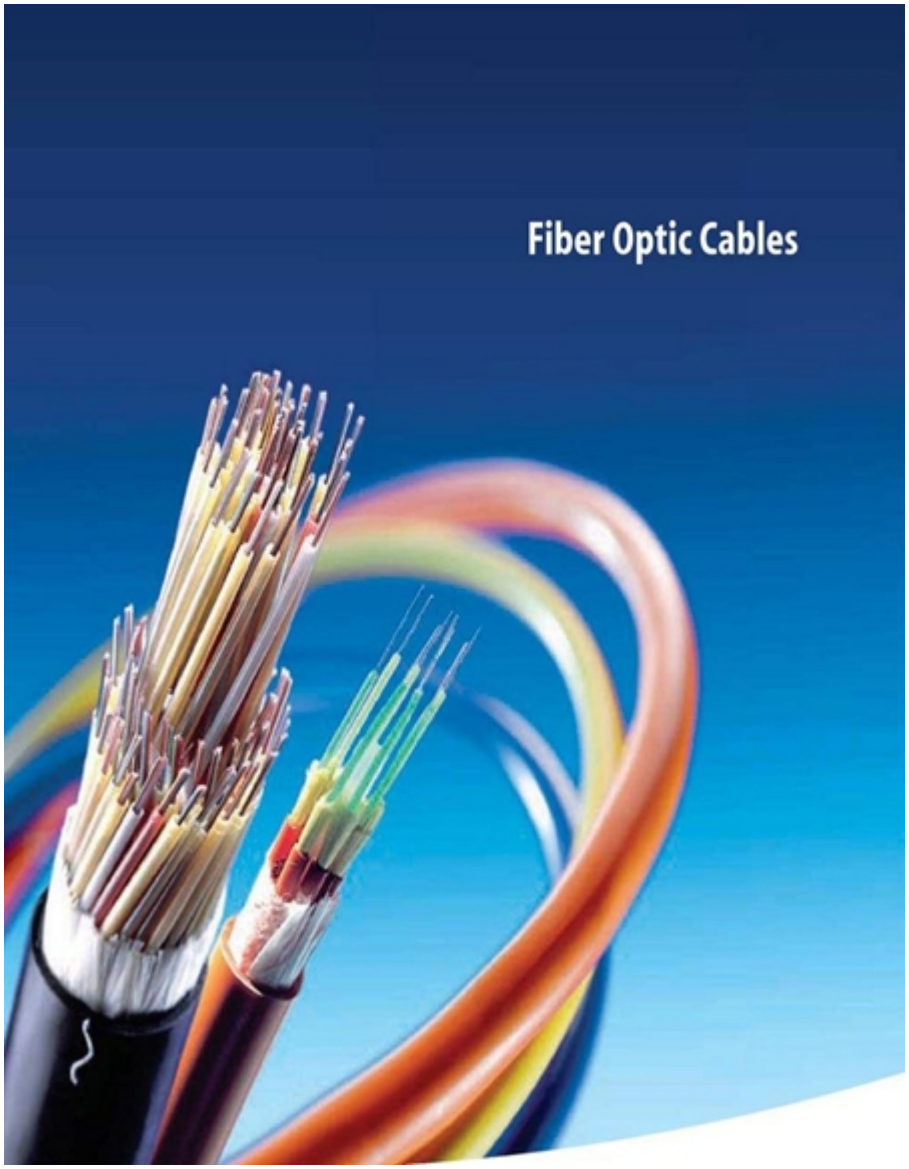
Licensed to Berend Post berend.post@it-university.nl

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

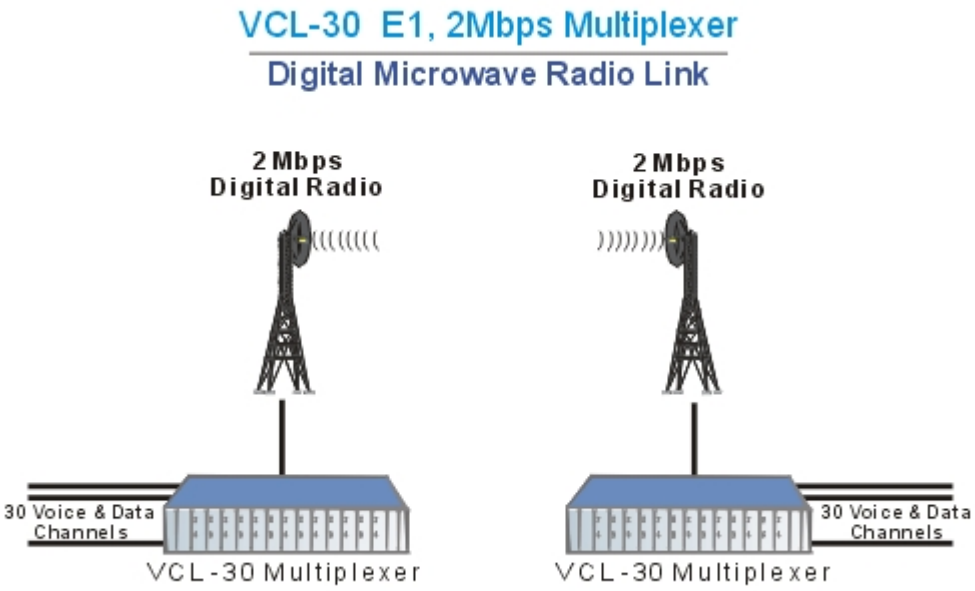
Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

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.

Reference:

CISA review manual 2014 page number 265

Question 867

Which of the following BEST determines if a batch update job was completed?

- ☐ Reviewing the job log
- ☒ Testing a sample of transactions
- ☐ Reviewing a copy of the script
- ☐ Obtaining process owner confirmation

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

Question 868

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

Question 869

A comprehensive IS audit policy should include guidelines detailing what involvement the internal audit team should have?

- ☐ in the development and coding of major OS applications.
- ☐ in the acquisition and maintenance of major WEB applications.
- ☐ in the human resource management cycle of the application development project.
- ☒ in the development, acquisition, conversion, and testing of major applications.
- ☐ None of the choices.

Explanation:

Explanation:

The audit policy should include guidelines detailing what involvement internal audit will have in the development, acquisition, conversion, and testing of major applications. Such a policy must be approved by top management for it to be effective.

Question 870

Human error is being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☐ DDoS
- ☐ ATP
- ☒ Social Engineering
- ☐ None of the choices.

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

Question 871

A 5-year audit plan provides for general audits every year and application audits on alternating years. To achieve higher efficiency, the IS audit manager would MOST likely:

- ☐ proceed with the plan and integrate all new applications.
- ☐ alternate between control self-assessment (CSA) and general audits every year.
- ☐ implement risk assessment criteria to determine audit priorities.
- ☒ have control self-assessments (CSAs) and formal audits of applications on alternating years.

Question 872

An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:

- ☐ the training needs for users after applying the patch.
- ☐ any beneficial impact of the patch on the operational systems.
- ☒ delaying deployment until testing the impact of the patch.
- ☐ the necessity of advising end users of new patches.

Explanation:

Explanation:

Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

Question 873

An IS auditor is assessing an organization's data loss prevention (DLP) solution for protecting intellectual property from insider theft. Which of the following would the auditor consider MOST important for effective data protection?

- ☐ Employee training on information handling
- ☒ Creation of DLP policies and procedures
- ☐ Encryption of data copied to flash drives
- ☐ Identification and classification of sensitive data

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

Question 874

What should be the information security manager's MOST important consideration when planning a disaster recovery test?

- ☐ Stakeholder notification procedures
- ☐ Organization-wide involvement
- ☒ Impact to production systems
- ☐ Documented escalation processes

Question 875

Which of the following provides the framework for designing and developing logical access controls?

- ☒ Information systems security policy
- ☐ Access control lists
- ☐ Password management
- ☐ System configuration files

Explanation:

Explanation:

The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control lists, password management and systems configuration files are tools for implementing the access controls.

Question 876

What should IS auditors always check when auditing password files?

- ☐ That deleting password files is protected
- ☒ That password files are encrypted
- ☐ That password files are not accessible over the network
- ☐ That password files are archived

Explanation:

Explanation:

IS auditors should always check to ensure that password files are encrypted.

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

Question 877

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:

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.

Reference:

CISA review manual 2014 Page number 215

Question 878

Which of the following attack involves slicing small amount of money from a computerize transaction or account?

- ☐ Eavesdropping
- ☐ Traffic Analysis
- ☒ Salami
- ☐ Masquerading

Explanation:

Explanation:

Salami slicing or Salami attack refers to a series of many small actions, often performed by clandestine means, that as an accumulated whole produces a much larger action or result that would be difficult or unlawful to perform all at once. The term is typically used pejoratively. Although salami slicing is often used to carry out illegal activities, it is only a strategy for gaining an advantage over time by accumulating it in small increments, so it can be used in perfectly legal ways as well.

An example of salami slicing, also known as penny shaving, is the fraudulent practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to the nearest cent (or other monetary unit) in financial transactions. It would be done by always rounding down, and putting the fractions of a cent into another account. The idea is to make the change small enough that any single transaction will go undetected.

In information security, a salami attack is a series of minor attacks that together results in a larger attack. Computers are ideally suited to automating this type of attack.

The following answers are incorrect:

 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.

Reference:

http://searchfinancialsecurity.techtarget.com/definition/eavesdropping

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

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 879

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 880

In a data center audit, an IS auditor finds that the humidity level is very low. The IS auditor would be MOST concerned because of an expected increase in:

- ☐ employee discomfort
- ☐ risk of fire
- ☒ static electricity problems
- ☐ backup tape failures

Question 881

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:

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.

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

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.

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:

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

The other types of IDS mentioned in the options do not resides on important systems like database and critical servers

Reference:

CISA review manual 2014 Page number 346 and 347

Question 882

Which of the following will MOST likely compromise the control provided by a digital signature created using RSA encryption?

- ☐ Deciphering the receiver's public key
- ☒ Obtaining the sender's private key
- ☐ Altering the plaintext message
- ☐ Reversing the hash function using the digest

Question 883

An organization migrated most of its physical servers to virtual ones in its own data center. Which of the following should be of GREATEST concern to an IS auditor reviewing the virtual environment?

- ☐ Hypervisor access control lists are outdated.
- ☐ The configuration management database (CMDB) does not include all virtual machines.
- ☐ Hypervisors have not been updated with the most recent patches.
- ☒ Virtual machine deployments are done without following an approved template.

Question 884

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.

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

Question 885

Validated digital signatures in an e-mail software application will:

- ☒ help detect spam.
- ☐ provide confidentiality.
- ☐ add to the workload of gateway servers.
- ☐ significantly reduce available bandwidth.

Explanation:

Explanation:

Validated electronic signatures are based on qualified certificates that are created by a certification authority (CA), with the technical standards required to ensure the key can neither be forced nor reproduced in a reasonable time. Such certificates are only delivered through a registration authority (RA) after a proof of identity has been passed. Using strong signatures in e- mail traffic, nonrepudiation can be assured and a sender can be tracked. The recipient can configure their e-mail server or client to automatically delete e-mails from specific senders. For confidentiality issues, one must use encryption, not a signature, although both methods can be based on qualified certificates. Without any filters directly applied on mail gateway servers to block traffic without strong signatures, the workload will not increase. Using filters directly on a gateway server will result in an overhead less than antivirus software imposes. Digital signatures are only a few bytes in size and will not slash bandwidth. Even if gateway servers were to check CRLs, there is little overhead.

Question 886

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 887

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 888

What is wrong with a Black Box type of intrusion detection system?

- ☐ you cannot patch it
- ☐ you cannot test it
- ☒ you cannot examine its internal workings from outside.
- ☐ you cannot tune it
- ☐ None of the choices.

Explanation:

Explanation:

"An intrusion detection system should be able to run continually without human supervision. The system must be reliable enough to allow it to run in the background of the system being observed. However, it should not be a "black box", because you want to ensure its internal workings are examinable from outside."

Question 889

A web organization is developed in-house by an organization. Which of the following would provide the BEST evidence to an IS auditor that the application is secure from external attack?

- ☐ Code review by a third party
- ☐ Web application firewall implementation
- ☒ Penetration test results
- ☐ Database application monitoring logs

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

Question 890

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 891

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

- ☒ The risks associated with the use of the products are periodically assessed
- ☐ The latest version of software is listed for each product
- ☐ Due to licensing issues the list does not contain open source software
- ☐ After hours' support is offered

Explanation:

Explanation:

Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C and D are possible considerations but would not be the most important.

Question 892

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 893

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 894

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 895

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

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

Explanation:

Explanation:

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

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

Question 896

Which of the following is the GREATEST advantage of implementing an IT enterprise architecture framework within an organization?

- ☒ It helps to identify security issues in systems across the organization.
- ☐ It better equips an organization to adopt innovative and emerging technologies.
- ☐ It reduces the overlap of infrastructure technologies within the organization.
- ☐ It improves the organization's ability to meet service level agreements (SLAs).

Question 897

Who is primarily responsible for storing and safeguarding the data?

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

Explanation:

Explanation:

Data Steward or data custodian is responsible for storing and safeguarding the data, and include IS personnel such as system analyst and computer operators.

For CISA exam you should know below roles in an organization

Data Owners – These peoples are generally managers and directors responsible for using information for running and controlling the business. Their security responsibilities include authorizing access, ensuring that access rules are updated when personnel changes occur, and regularly review access rule for the data for which they are responsible.

Data Custodian or Data Steward – These people are responsible for storing and safeguarding the data, and include IS personnel such as system analysis and computer operators.

Security Administrator -Security administrator is responsible for providing adequate physical and logical security for IS programs, data and equipment.

Data Users – Data users, including internal and external user community, are the actual user of computerized data. Their level of access into the computer should be authorized by data owners, and restricted and monitor by security administrator.

The following were incorrect answers:

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

Data Owner- These peoples are generally managers and directors responsible for using information for running and controlling the business.

Data Users – Data users, including internal and external user community, are the actual user of computerized data.

Security Administrator - Security administrator is responsible for providing adequate and logical security for IS programs, data and equipment.

Reference:

CISA review manual 2014 Page number361

Question 898

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 899

The PRIMARY advantage of object-oriented technology is enhanced:

- ☒ efficiency due to the re-use of elements of logic.
- ☐ management of sequential program execution for data access.
- ☐ management of a restricted variety of data types for a data object.
- ☐ grouping of objects into methods for data access.

Question 900

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:

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

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.

Question 901

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 902

In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

- ☐ CASE tools
- ☐ Embedded data collection tools
- ☐ Heuristic scanning tools
- ☒ Trend/variance detection tools

Explanation:

Explanation:

Trend/variance detection tools look for anomalies in user or system behavior, for example, determining whether the numbers for prenumbered documents are sequential or increasing. CASE tools are used to assist software development. Embedded (audit) data collection software is used for sampling and to provide production statistics. Heuristic scanning tools can be used to scan for viruses to indicate possible infected code.

Question 903

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

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

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

Question 904

A critical function of a firewall is to act as a:

- ☐ special router that connects the Internet to a LAN.
- ☒ device for preventing authorized users from accessing the LAN.
- ☐ server used to connect authorized users to private trusted network resources.
- ☐ proxy server to increase the speed of access to authorized users.

Explanation:

Explanation:

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

Question 905

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:

Explanation:

In phased changeover approach, the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.

Some of the risk areas that may exist in the phased changeover area includes:

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

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.

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.

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

Reference:

CISA review manual 2014 Page number 172

Question 906

Which of the following would be an auditor's GREATEST concern when reviewing data inputs from spreadsheets into the core finance system?

- ☒ Undocumented code formats data and transmits directly to the database.
- ☐ There is not a complete inventory of spreadsheets, and file naming is inconsistent.
- ☐ Spreadsheets are accessible by all members of the finance department.
- ☐ The department data protection policy has not been reviewed or updated for two years.

Question 907

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 908

In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

- ☒ Approve and document the change the next business day
- ☐ Limit developer access to production to a specific timeframe
- ☐ Obtain secondary approval before releasing to production
- ☐ Disable the compiler option in the production machine

Explanation:

Explanation:

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

It may be appropriate to allow programmers to make emergency changes as long as they are documented and approved after the fact. Restricting release time frame may help somewhat; however, it would not apply to emergency changes and cannot prevent unauthorized release of the programs. Choices C and D are not relevant in an emergency situation.

Question 909

During a post-incident review of a security breach, what type of analysis should an IS auditor expect to be performed by the organization's information security team?

- ☐ Gap analysis
- ☒ Business impact analysis (BIA)
- ☐ Qualitative risk analysis
- ☐ Root cause analysis

Question 910

An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

- ☐ Controls the proliferation of multiple versions of programs
- ☒ Expands the programming resources and aids available
- ☐ Increases program and processing integrity
- ☐ Prevents valid changes from being overwritten by other changes

Explanation:

Explanation:

A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

Question 911

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

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

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 912

Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- ☒ Review the parameter settings.
- ☐ Interview the firewall administrator.
- ☐ Review the actual procedures.
- ☐ Review the device's log file for recent attacks.

Explanation:

Explanation:

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide audit evidence as strong as choice A.

Question 913

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 914

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 915

Which of the following is a general operating system access control function?

- ☐ Creating database profiles
- ☐ Verifying user authorization at a field level
- ☒ Creating individual accountability
- ☐ Logging database access activities for monitoring access violation

Explanation:

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

Explanation:

Creating individual accountability is the function of the general operating system. Creating database profiles, verifying user authorization at a field level and logging database access activities for monitoring access violations are all database-level access control functions.

Question 916

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

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

Explanation:

Explanation:

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

For your exam you should know the information below:

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,

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

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

Website forgery

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

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

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.

Reference:

CISA review manual 2014 Page number 323

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

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

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

Question 917

Which of the following is a benefit of requiring management to issue a report to stakeholders regarding the internal controls over IT?

- ☐ Transparency of IT costs
- ☐ Improved portfolio management
- ☐ Improved cost management
- ☒ Focus on IT governance

Question 918

Which of the following is an indication of possible hacker activity involving voice communications?

- ☐ A significant percentage of lines are busy during early morning and late afternoon hours.
- ☒ Outbound calls are found to significantly increase in frequency during non-business hours.
- ☐ Inbound calls experience significant fluctuations based on time-of-day and day-of-week.
- ☐ Direct inward system access (DISA) is found to be disabled on the company's exchange.

Question 919

During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

- ☒ buffer overflow.
- ☐ brute force attack.
- ☐ distributed denial-of-service attack.
- ☐ war dialing attack.

Explanation:

Explanation:

Poorly written code, especially in web-based applications, is often exploited by hackers using buffer overflow techniques. A brute force attack is used to crack passwords. A distributed denial- of-service attack floods its target with numerous packets, to prevent it from responding to legitimate requests. War dialing uses modem-scanning tools to hack PBXs.

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

Question 920

An organization implemented a mandatory information security awareness training program a year ago. What is the BEST way to determine its effectiveness?

- ☐ Analyze responses from an employee survey on training satisfaction.
- ☐ Analyze results from training completion reports.
- ☒ Analyze results of a social engineering test.
- ☐ Analyze findings from previous audit reports.

Question 921

Which of the following is the most important benefit of control self-assessment (CSA)?

- ☐ CSA is a policy/rule driven
- ☒ In CSA approach, risk is identified sooner
- ☐ CSA requires limited employee participations
- ☐ In CSA, resources are being used in an effective manner.

Explanation:

Explanation:

Control self-assessment is an assessment of controls made by staff and management within the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal controls of the organization are reliable. The CSA approach requires extensive employee participations and training. This will help to employee understand more about business risks. This will insure the detection of risk in timely manner.

For your exam you should know the information below about control self-assessment:

Benefits of CSA

Early detection of risk

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives

Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

Highly motivated employees

Improved audit training process

Reduction in control cost

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

Assurance provided to stakeholders and customers

Traditional and CSA attributes

Traditional Historical CSA

Assign duties/supervises staff Empowered/accountable employees

Policy/rule driven Continuous improvement/learning curve

Limited employee participation Extensive employee participation and training

Narrow stakeholders focus Broad stakeholders focus

Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are incorrectly describes about CSA.

Reference:

CISA review manual 2014 page number 61, 62 and 63

Question 922

Which of the following activities provides an IS auditor with the MOST insight regarding potential single person dependencies that might exist withing the organization?

- ☐ Reviewing user activity logs
- ☐ Mapping IT processes to roles
- ☒ Reviewing vacation patterns
- ☐ Interviewing senior IT management

Question 923

Which of the following is necessary for the effective risk management in IT governance?

- ☒ Risk evaluation is embedded in management processes
- ☐ Risk management strategy is approved by the audit committee
- ☐ Local managers are solely responsible for risk evaluation
- ☐ IT risk management is separate from corporate risk management

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

Question 924

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

Question 925

Which of the following should be the MOST important consideration when establishing data classification standards?

- ☐ An education campaign is established upon rollout.
- ☐ Reporting metrics are established.
- ☒ Management supports the newly developed standards.
- ☐ The standards comply with relevant regulations.

Question 926

Which of the following database model allow many-to-many relationships in a tree-like structure that allows multiple parents?

- ☐ Hierarchical database model
- ☒ Network database model
- ☐ Relational database model
- ☐ Object-relational database model

Explanation:

Explanation:

Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

For your exam you should know below information about database models:

A database model is a type of data model that determines the logical structure of a database and fundamentally determines in which manner data can be stored, organized, and manipulated. The most popular example of a database model is the relational model, which uses a table-based format.

Common logical data models for databases include:

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

Hierarchical database model

Network model

Relational model

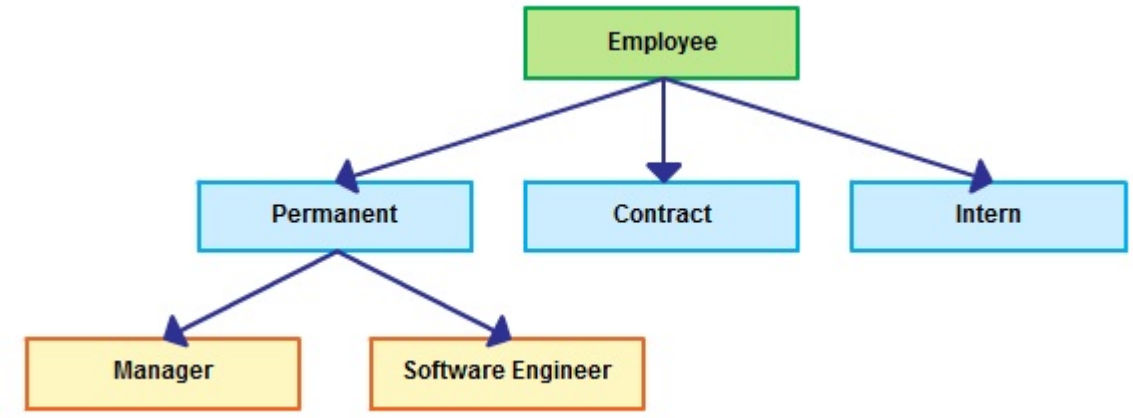
Object-relational database models

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



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.

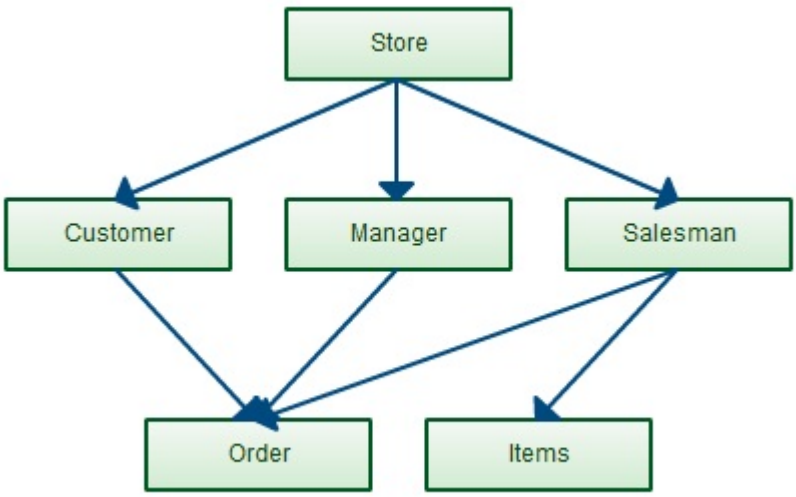
Licensed to Berend Post berend.post@it-university.nl

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



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.

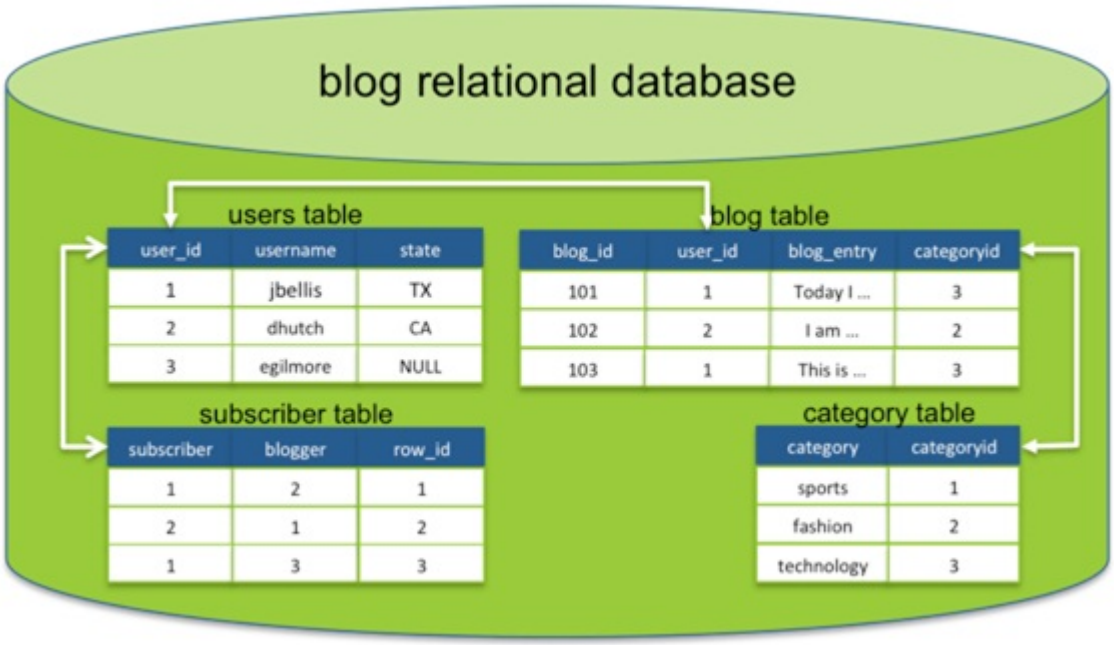
Licensed to Berend Post berend.post@it-university.nl

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



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

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

An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

The following were incorrect answers:

Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

Relational model- In the relational model of a database, all data is represented in terms of tulles, grouped into relations. A database organized in terms of the relational model is a relational database. In the relational model, related records are linked together with a "key".

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are 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.

Reference:

CISA review manual 2014 Page number 254

Question 927

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

- ☐ Sag
- ☐ Blackout
- ☒ Brownout
- ☐ EMI

Explanation:

Explanation:

The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

For CISA exam you should know below information about power failure

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

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Sags, spike and surge – Temporary and rapid decreases (sag) or increases (spike and surges) in a voltage levels. These anomalies can cause loss of data, data corruption, network transmission errors or physical damage to hardware devices.

Electromagnetic interference (EMI) - The electromagnetic interference (EMI) caused by electrical storms or noisy electrical equipments. The interference may cause computer system to hang or crash as well as damages similar to those caused by sags, spike and surges.

The following were incorrect answers:

Sag – Temporarily rapid decrease in a voltage.

Total Failure (Blackout) – A complete loss of electric power, which may span from a single building to an entire geographical are and is often caused by weather conditions or inability of an electric utility company to meet user demands

Severely reduced voltage (brownout) – The failure of an electric utility company to supply power within acceptable range. Such a failure places a strain on electronic equipment and may limit their operational life or even cause permanent damage.

Reference:

CISA review manual 2014 Page number372

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

Question 928

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- ☒ Modems convert analog transmissions to digital, and digital transmission to analog.
- ☐ Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
- ☐ Modems convert digital transmissions to analog, and analog transmissions to digital.
- ☐ Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Explanation:

Explanation:

Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

Question 929

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

- ☐ Use of a cryptographic hashing algorithm
- ☐ Enciphering the message digest
- ☐ Deciphering the message digest
- ☒ A sequence number and time stamp

Explanation:

Explanation:

When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection, and could be used to verify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

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

Question 930

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 931

The MAIN objective of incident management is to:

- ☐ have an external computer security incident response team assess damage.
- ☐ permit the incident to go on and follow the trail back to the beginning.
- ☒ test for readiness to respond when facing an incident.
- ☐ keep the business going while the response is occurring.

Question 932

While reviewing similar issues in an organization's help desk system, an IS auditor finds that they were analyzed independently and resolved differently. This situation MOST likely indicates a deficiency in:

- ☐ IT service level management.
- ☐ change management.
- ☐ configuration management.
- ☒ problem management.

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

Question 933

An organization uses electronic funds transfer (EFT) to pay its vendors. Which of the following should be an IS auditor's MAIN focus while reviewing controls in the accounts payable application?

- ☒ Changes to the vendor master file
- ☐ Volume of transactions
- ☐ Amount of disbursements
- ☐ Frequency of transactions

Question 934

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 935

Which of the following provides nonrepudiation services for e-commerce transactions?

- ☒ Public key infrastructure (PKI)
- ☐ Data Encryption Standard (DES)
- ☐ Message authentication code (MAC)
- ☐ Personal identification number (PIN)

Explanation:

Explanation: PKI is the administrative infrastructure for digital certificates and encryption key pairs. The qualities of an acceptable digital signature are: it is unique to the person using it; it is capable of verification; it is under the sole control of the person using it; and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The Data Encryption Standard (DES) is the most common private key cryptographic system. DES does not address nonrepudiation. A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission; it has nothing to do with nonrepudiation. A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

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

Question 936

Involvement of senior management is MOST important in the development of:

- ☒ strategic plans.
- ☐ IS policies.
- ☐ IS procedures.
- ☐ standards and guidelines.

Explanation:

Explanation:

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

Question 937

Which of the following acts as a decoy to detect active internet attacks?

- ☒ Honeypots
- ☐ Firewalls
- ☐ Trapdoors
- ☐ Traffic analysis

Explanation:

Explanation:

Honeypots are computer systems that are expressly set up to attract and trap individuals who attempt to penetrate other individuals' computer systems. The concept of a honeypot is to learn from intruder's actions. A properly designed and configured honeypot provides data on methods used to attack systems. The data are then used to improve measures that could curb future attacks. A firewall is basically a preventive measure. Trapdoors create a vulnerability that provides an opportunity for the insertion of unauthorized code into a system. Traffic analysis is a type of passive attack.

Question 938

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.

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

Question 939

Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

- ☐ Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
- ☐ Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables.
- ☒ Extrapolation of the overall end date based on completed work packages and current resources
- ☐ Calculation of the expected end date based on current resources and remaining available project budget

Explanation:

Explanation:

Direct observation of results is better than estimations and qualitative information gained from interviews or status reports. Project managers and involved staff tend to underestimate the time needed for completion and the necessary time buffers for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

Question 940

Before concluding that internal controls can be relied upon, the IS auditor should:

- ☐ discuss the internal control weaknesses with the auditee
- ☐ document application controls
- ☒ conduct tests of compliance
- ☐ document the system of internal control

Question 941

Which of the following should an IS auditor use when verifying a three-way match has occurred in an enterprise resource planning (ERP) system?

- ☐ Goods delivery notification
- ☐ Purchase requisition
- ☐ Bank confirmation
- ☒ Purchase order

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

Question 942

Which of the following should be of MOST concern to an IS auditor reviewing an organization's disaster recovery plan (DRP)?

- ☐ The responsibility for declaring a disaster is not identified.
- ☒ The disaster recovery steps are not detailed.
- ☐ The CIO has not signed off on the DRP.
- ☐ Copies of the DRP are not kept in a secure offsite location.

Question 943

Which of the following testing approaches provides the GREATEST assurance that only approved systems development releases have been implemented in the production environment?

- ☐ Test whether a sample of approved developments have releases in production migration logs.
- ☐ Test whether a sample of developments in the systems development register have documented approvals.
- ☒ Test whether a sample of releases in production migration logs have corresponding approvals.
- ☐ Test whether a sample of releases followed the organization's segregation of duties access.

Question 944

An IS auditor is asked to provide feedback on the systems options analysis for a new project. The BEST course of action for the IS auditor would be to:

- ☐ identify the best alternative.
- ☐ request at least one other alternative.
- ☒ comment on the criteria used to assess the alternatives.
- ☐ retain comments as findings for the audit report.

Question 945

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 cannot be altered. Depending on the mechanism chosen to implement a digital signature, the

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

mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

Question 946

While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern should be that the:

- ☒ requirement for protecting confidentiality of information could be compromised.
- ☐ contract may be terminated because prior permission from the outsourcer was not obtained.
- ☐ other service provider to whom work has been outsourced is not subject to audit.
- ☐ outsourcer will approach the other service provider directly for further work.

Explanation:

Explanation:

Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are no related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

Question 947

Which of the following testing method examines internal structure or working of an application?

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

Explanation:

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).

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

White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system–level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements.

For your exam you should know the information below:

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

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

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.

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.

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

The following answers are incorrect:

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

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

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

Reference:

CISA review manual 2014 Page number 167

Official ISC2 guide to CISSP CBK 3rd Edition Page number 176

Question 948

Which of the following is used in providing logical access control to restrict updating or deleting business information in a relational database?

- ☐ Trigger
- ☒ View
- ☐ Join
- ☐ Primary key

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

Question 949

What is the FIRST line of defense against criminal insider activities?

- ☐ Validating the integrity of personnel
- ☐ Monitoring employee activities
- ☐ Signing security agreements by critical personnel
- ☒ Stringent and enforced access controls

Question 950

To overcome the perception that security is a hindrance to business activities, it is important for an information security manager to:

- ☐ rely on senior management to enforce security
- ☒ promote the relevance and contribution of security
- ☐ reiterate the necessity of security
- ☐ focus on compliance

Question 951

The PRIMARY objective of service-level management (SLM) is to:

- ☒ define, agree, record and manage the required levels of service.
- ☐ ensure that services are managed to deliver the highest achievable level of availability.
- ☐ keep the costs associated with any service at a minimum.
- ☐ monitor and report any legal noncompliance to business management.

Explanation:

Explanation:

The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services. This does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level, since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

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

Question 952

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.

Question 953

The BEST way to avoid session hijacking is to use:

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

Question 954

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:

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.

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

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

Reference:

CISA review manual 2014 Page number 348

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

http://www.ce-infosys.com/english/free_compusec/free_compusec.aspx

Question 955

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

- ☐ Process maturity
- ☐ Performance indicators
- ☒ Business risk
- ☐ Assurance reports

Explanation:

Explanation:

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

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

Question 956

Which of the following provides the GREATEST assurance that any confidential information on a disk is no longer accessible but the device is still usable by other internal users?

- ☒ Reformatting the disk
- ☐ Erasing the disk
- ☐ Degaussing the disk
- ☐ Password-protecting the disk

Question 957

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 958

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

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

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 959

In an online application, which of the following would provide the MOST information about the transaction audit trail?

- ☐ File layouts
- ☒ System/process flowchart
- ☐ Source code documentation
- ☐ Data architecture

Question 960

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 961

Which of the following is the BEST way to mitigate the impact of ransomware attacks?

- ☒ Backing up data frequently
- ☐ Invoking the disaster recovery plan (DRP)
- ☐ Requiring password changes for administrative accounts
- ☐ Paying the ransom

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

Question 962

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:

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 963

Which is MOST important when contracting an external party to perform a penetration test?

- ☐ Obtain approval from IT management.
- ☒ Define the project scope.
- ☐ Increase the frequency of log reviews.
- ☐ Provide network documentation.

Question 964

Which of the following audit risk is related to material errors or misstatements that have occurred that will not be detected by an IS auditor?

- ☐ Inherent Risk
- ☐ Control Risk
- ☒ Detection Risk
- ☐ Overall Audit Risk

Explanation:

Explanation:

The risk that material errors or misstatements that have occurred will not be detected by an IS auditor. Detection Risk is the risk that the auditors fail to detect a material misstatement in the financial statements. An auditor must apply audit procedures to detect material misstatements in the financial statements whether due to fraud or error. Misapplication or omission of critical audit

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

procedures may result in a material misstatement remaining undetected by the auditor. Some detection risk is always present due to the inherent limitations of the audit such as the use of sampling for the selection of transactions. Detection risk can be reduced by auditors by increasing the number of sampled transactions for detailed testing.

For your exam you should know below information about audit risk:

Audit risk (also referred to as residual risk) refers to the risk that an auditor may issue unqualified report due to the auditor's failure to detect material misstatement either due to error or fraud. This risk is composed of inherent risk (IR), control risk (CR) and detection risk (DR), and can be calculated thus:

AR = IR • CR • DR

Inherent Risk

Auditors must determine risks when working with clients. One type of risk to be aware of is inherent risk. While assessing this level of risk, you ignore whether the client has internal controls in place (such as a secondary review of financial statements) in order to help mitigate the inherent risk. You consider the strength of the internal controls when assessing the client's control risk. Your job when assessing inherent risk is to evaluate how susceptible the financial statement assertions are to material misstatement given the nature of the client's business. A few key factors can increase inherent risk.

Environment and external factors: Here are some examples of environment and external factors that can lead to high inherent risk:

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

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

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.

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:

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

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:

Inherent Risk - It is the risk level or exposure of a process or entity to be audited without taking into account the control that management has implemented.

Control Risk - The risk that material error exist that would not be prevented or detected on timely basis by the system of internal controls.

Overall audit risk - The probability that information or financial report may contain material errors and that the auditor may not detect an error that has occurred. An objective in formulating the audit approach is to limit the audit risk in the area under security so the overall audit risk is at sufficiently low level at the completion of the examination.

Reference:

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

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 965

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 966

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

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

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 967

Which of the following is the MOST important element for the successful implementation of IT governance?

- ☐ Implementing an IT scorecard
- ☒ Identifying organizational strategies
- ☐ Performing a risk assessment
- ☐ Creating a formal security policy

Explanation:

Explanation:

The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices-even if implemented-would be ineffective.

Question 968

Which of the following is MOST important for an IS auditor to verify when reviewing a critical business application that requires high availability?

- ☐ Algorithms are reviewed to resolve process inefficiencies.
- ☐ Users participate in offsite business continuity testing.
- ☒ There is no single point of failure.
- ☐ Service level agreement (SLAs) are monitored.

Question 969

A new system development project is running late against a critical implementation deadline. Which of the following is the MOST important activity?

- ☐ Document last-minute enhancements.
- ☐ Perform user acceptance testing.
- ☐ Perform a pre-implementation audit.
- ☒ Ensure that code has been reviewed.

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

Question 970

Which of the following is MOST likely to be included in computer operating procedures in a large data center?

- ☒ Instructions for job scheduling
- ☐ Procedures for resequencing source code
- ☐ Procedures for utility configuration
- ☐ Guidance on setting security parameters

Question 971

The PRIMARY purpose of vulnerability assessments is to:

- ☒ detect deficiencies that could lead to a system compromise.
- ☐ provide clear evidence that the system is sufficiently secure.
- ☐ test intrusion detection systems (IDS) and response procedures.
- ☐ determine the impact of potential threats.

Question 972

Which of the following is MOST important to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings?

- ☐ Restricting evidence access to professionally certified forensic investigators
- ☐ Engaging an independent third party to perform the forensic investigation
- ☐ Performing investigative procedures on the original hard drives rather than images of the hard drives
- ☒ Documenting evidence handling by personnel throughout the forensic investigation

Question 973

Which of the following strategies BEST optimizes data storage without compromising data retention practices?

- ☐ Limiting the size of the file attachments being sent via email
- ☐ Automatically deleting emails older than one year
- ☒ Moving emails to a virtual email vault after 30 days
- ☐ Allowing employees to store large emails on flash drives

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

Question 974

The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

- ☐ that there will be too many alerts for system administrators to verify.
- ☐ decreased network performance due to IPS traffic.
- ☒ the blocking of critical systems or services due to false triggers.
- ☐ reliance on specialized expertise within the IT organization.

Explanation:

Explanation:

An intrusion prevention system (IPS) prevents a connection or service based on how it is programmed to react to specific incidents. If the packets are coming from a spoofed address and the IPS is triggered based on previously defined behavior, it may block the service or connection of a critical internal system. The other choices are risks that are not as severe as blocking critical systems or services due to false triggers.

Question 975

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

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

More efficient and improved internal controls

Creation of cohesive teams through employee involvement

Developing a sense of ownership of the controls in the employees and process owners, and reducing their resistance to control improvement initiatives

Increased employee awareness of organizational objectives, and knowledge of risk and internal controls

Highly motivated employees

Improved audit training process

Reduction in control cost

Assurance provided to stakeholders and customers

Traditional and CSA attributes

Traditional Historical CSA

Assign duties/supervises staff Empowered/accountable employees

Policy/rule driven Continuous improvement/learning curve

Limited employee participation Extensive employee participation and training

Narrow stakeholders focus Broad stakeholders focus

Auditors and other specialist Staff at all level, in all functions, are the primary control analysts

The following answers are incorrect:

The other options specified are correctly describes about CSA.

Reference:

CISA review manual 2014 page number 61, 62 and 63

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

Question 976

An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

- ☒ Denial-of-service
- ☐ Replay
- ☐ Social engineering
- ☐ Buffer overflow

Explanation:

Explanation:

Prior to launching a denial-of-service attack, hackers often use automatic port scanning software to acquire information about the subject of their attack. A replay attack is simply sending the same packet again. Social engineering exploits end-user vulnerabilities, and buffer overflow attacks exploit poorly written code.

Question 977

What is an IS auditor's BEST recommendation for management if a network vulnerability assessment confirms that critical patches have not been applied since the last assessment?

- ☒ Implement a process to test and apply appropriate patches.
- ☐ Apply available patches and continue periodic monitoring.
- ☐ Configure servers to automatically apply available patches.
- ☐ Remove unpatched devices from the network.

Question 978

Which of the following is the MOST effective data loss control when connecting a personally owned mobile device to the corporate email system?

- ☐ A senior manager must approve each new connection.
- ☐ Email synchronization must be prevented when connected to a public Wi-Fi hotspot.
- ☒ Email must be stored in an encrypted format on the mobile device.
- ☐ Users must agree to allow the mobile device to be wiped if it is lost.

Question 979

Which of the following layer of an OSI model encapsulates packets into frames?

- ☐ Transport Layer
- ☐ Network Layer
- ☒ Data Link Layer
- ☐ Physical Layer
- ☐ .

Explanation:

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

Explanation:

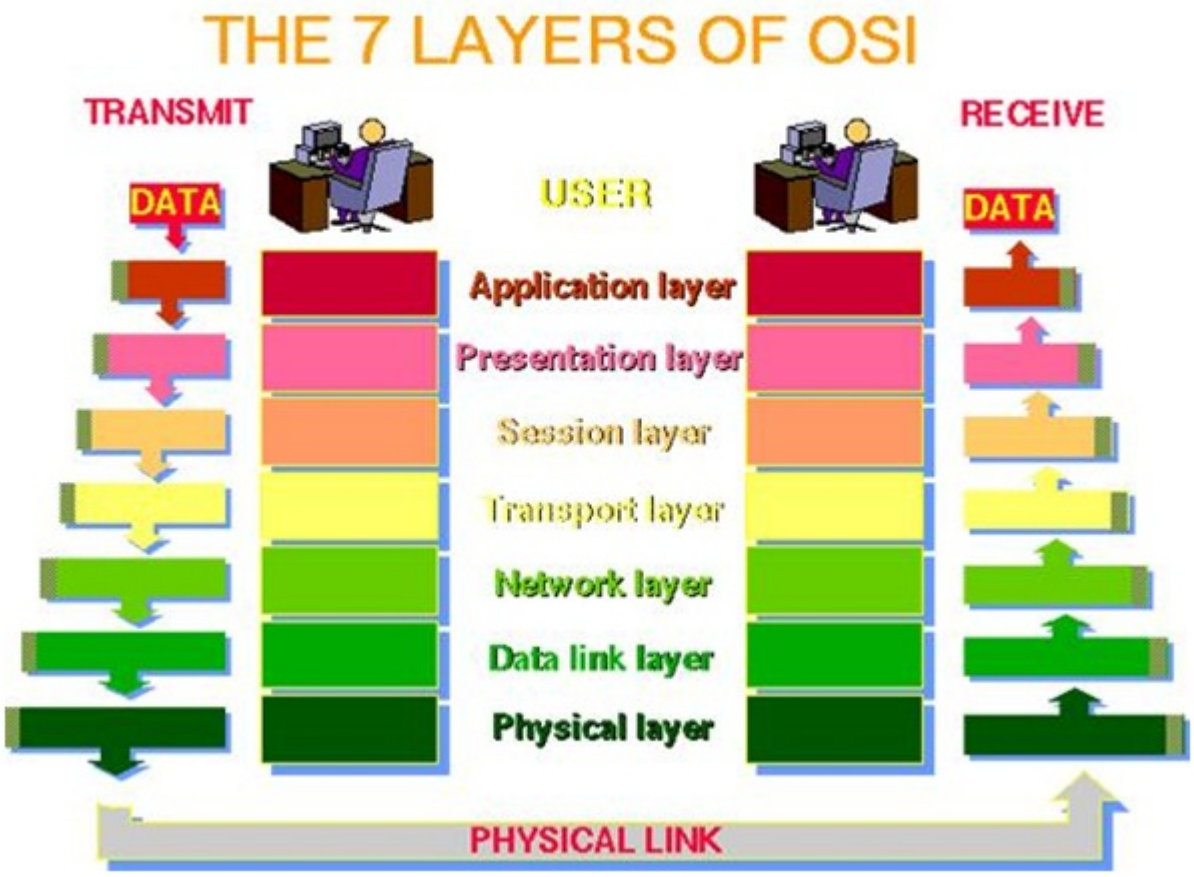
The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.

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

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

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

OSI Model



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

PHYSICAL LAYER

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

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

What signal state represents a binary 1

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

How the receiving station delimits a frame

DATA LINK LAYER

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

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.

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

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

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

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

Communications Subnet

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

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

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

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.

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

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

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

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

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

End-to-end layers

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

SESSION LAYER

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.

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

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.

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

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

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

APPLICATION LAYER

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

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

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

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

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

Reference:

CISA review manual 2014 Page number 260

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

Question 980

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 981

The lack of which of the following represents the GREATEST risk to the quality of developed software?

- ☒ Code reviews
- ☐ Periodic internal audits
- ☐ Load testing
- ☐ An enterprise architecture

Question 982

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

- ☒ increases in quality can be achieved, even if resource allocation is decreased.
- ☐ increases in quality are only achieved if resource allocation is increased.
- ☐ decreases in delivery time can be achieved, even if resource allocation is decreased.
- ☐ decreases in delivery time can only be achieved if quality is decreased.

Explanation:

Explanation:

The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

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

Question 983

Which of the following is MOST influential when defining disaster recovery strategies?

- ☐ Existing server redundancies
- ☒ Maximum tolerable downtime
- ☐ Data classification scheme
- ☐ Annual loss expectancy

Question 984

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 985

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.

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

Question 986

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 987

Which of the following audit assess accuracy of financial reporting?

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

Explanation:

Explanation:

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

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

What is an audit?

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

Compliance Audit

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

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

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

Financial Audit

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

Operational Audit

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

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

Objectives

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

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

To understand the responsibilities and risks faced by an organization.

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

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

Integrated Audits

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

IS Audit

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

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

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

Forensic Audit

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

The purpose of a forensic audit is to use accounting procedures to collect evidence for the prosecution or investigation of financial crimes such as theft or fraud. Forensic audits may be

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

conducted to determine if wrongdoing occurred, or to gather materials for the case against an alleged criminal.

The following answers are incorrect:

Compliance Audit - A compliance audit is a comprehensive review of an organization's adherence to regulatory guidelines. Independent accounting, security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, user access controls and risk management procedures over the course of a compliance audit. Compliance audit include specific tests of controls to demonstrate adherence to specific regulatory or industry standard. These audits often overlap traditional audits, but may focus on particular system or data.

Operational Audit - Operational Audit is a systematic review of effectiveness, efficiency and economy of operation. Operational audit is a future-oriented, systematic, and independent evaluation of organizational activities. In Operational audit financial data may be used, but the primary sources of evidence are the operational policies and achievements related to organizational objectives.[1] Operational audit is a more comprehensive form of an Internal audit.

Forensic Audit - Forensic audit is the activity that consists of gathering, verifying, processing, analyzing of and reporting on data in order to obtain facts and/or evidence - in a predefined context - in the area of legal/financial disputes and or irregularities (including fraud) and giving preventative advice.

Reference:

CISA Review Manual 2014 Page number 44

http://searchcompliance.techtarget.com/definition/compliance-audit

http://en.wikipedia.org/wiki/Financial_audit

http://en.wikipedia.org/wiki/Operational_auditing

http://en.wikipedia.org/wiki/Information_technology_audit

http://www.investorwords.com/16445/forensic_audit.html

Licensed to Berend Post berend.post@it-university.nl

Question 988

Phishing attack works primarily through:

- ☒ email and hyperlinks
- ☐ SMS
- ☐ chat
- ☐ email attachment
- ☐ news
- ☐ file download
- ☐ None of the choices.

Explanation:

Explanation:

"Phishing applies to email appearing to come from a legitimate business, requesting "verification"" of information and warning of some dire consequence if it is not done. The letter usually contains a link to a fradulent web page that looks legitimate and has a form requesting everything from a home address to an ATM card's PIN."

Question 989

An IS auditor discovers an option in a database that allows the administrator to directly modify any table. This option is necessary to overcome bugs in the software, but is rarely used. Changes to tables are automatically logged. The IS auditor's FIRST action should be to:

- ☐ determine whether the log of changes to the tables is backed up.
- ☒ determine whether the audit trail is secured and reviewed.
- ☐ recommend that the option to directly modify the database be removed immediately.
- ☐ recommend that the system require two persons to be involved in modifying the database.

Question 990

An IS auditor finds that corporate mobile devices used by employees have varying levels of password settings. Which of the following would be the BEST recommendation?

- ☐ Update the acceptable use policy for mobile devices.
- ☐ Notify employees to set passwords to a specified length.
- ☐ Encrypt data between corporate gateway and devices.
- ☒ Apply a security policy to the mobile devices.

Licensed to Berend Post berend.post@it-university.nl

Question 991

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 992

Which of the following will provide the GREATEST assurance to IT management that a quality management system (QMS) is effective?

- ☒ A high percentage of incidents being quickly resolved
- ☐ A high percentage of stakeholders satisfied with the quality of IT
- ☐ A high percentage of IT processes reviewed by quality assurance
- ☐ A high percentage of IT employees attending quality training

Question 993

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 994

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

Licensed to Berend Post berend.post@it-university.nl

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 995

Which of the following is MOST likely to result from a business process reengineering (BPR) Project?

- ☒ An increased number of people using technology
- ☐ Significant cost saving, through a reduction the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Explanation:

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:

B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.

D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

Question 996

Which of the following activities would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA)?

- ☒ Developing the CSA questionnaire
- ☐ Developing the remediation plan
- ☐ Implementing the remediation plan
- ☐ Partially completing the CSA

Question 997

Which of the following would provide the MOST useful input to IS audit management when developing an action plan for improving internal audit's performance?

- ☐ Feedback from departments that have participated in IS audits
- ☐ Industry benchmarking analysis
- ☐ An external quality assessment review
- ☒ Results train an improvement initiative overseen by executive management

Licensed to Berend Post berend.post@it-university.nl

Question 998

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 999

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 1000

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

Licensed to Berend Post berend.post@it-university.nl

then focus on business logic. The other choices are not the most significant advantages of a component-based development approach.

Question 1001

Which of the following provides for the GREATEST cost reduction in a large data center?

- ☒ Server consolidation
- ☐ Staff rotation
- ☐ Power conditioning
- ☐ Job-scheduling software

Question 1002

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:

Explanation:

Parallel testing is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

For CISA exam you should know below mentioned types of testing

Alpha and Beta Testing – An alpha version is early version is an early version of the application system submitted to the internal user for testing. The alpha version may not contain all the features planned for the final version. Typically, software goes to two stages testing before it consider finished. The first stage is called alpha testing is often performed only by the user within the organization developing the software. The second stage is called beta testing, a form of user acceptance testing, generally involves a limited number of external users. Beta testing is the last stage of testing, and normally involves real world exposure, sending the beta version of the product to independent beta test sites or offering it free to interested user.

Pilot Testing – A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities.

Licensed to Berend Post berend.post@it-university.nl

White box testing – Assess the effectiveness of a software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's specific logic path. However, testing all possible logical path in large information system is not feasible and would be cost prohibitive, and therefore is used on selective basis only.

Black Box Testing – An integrity based form of testing associated with testing components of an information system's "functional" operating effectiveness without regards to any specific internal program structure. Applicable to integration and user acceptance testing.

Function/validation testing – It is similar to system testing but it is often used to test the functionality of the system against the detailed requirements to ensure that the software that has been built is traceable to customer requirements.

Regression Testing – The process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

Parallel Testing – This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

Sociability Testing – The purpose of these tests is to confirm that new or modified system can operate in its target environment without adversely impacting existing system. This should cover not only platform that will perform primary application processing and interface with other system but, in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs) , making operating system registry or configuration file modification, and possibly extra memory utilization.

The following 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.

Licensed to Berend Post berend.post@it-university.nl

Pilot Testing – A preliminary test that focuses on specific and predefined aspect of a system. It is not meant to replace other testing methods, but rather to provide a limited evaluation of the system. Proof of concept are early pilot tests – usually over interim platform and with only basic functionalities

Reference:

CISA review manual 2014 Page number 167

Question 1003

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 1004

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:

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

 Licensed to Berend Post berend.post@it-university.nl

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

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).

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

CISA review manual 2014 Page number355

Question 1005

Which of the following is an advantage of the top-down approach to software testing?

- ☒ Interface errors are identified early
- ☐ Testing can be started before all programs are complete
- ☐ it is more effective than other testing approaches
- ☐ Errors in critical modules are detected sooner

Explanation:

Explanation:

The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner. The most effective testing approach is dependent on the environment being tested. Choices B and D are advantages of the bottom-up approach to system testing.

Licensed to Berend Post berend.post@it-university.nl

Question 1006

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 1007

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 1008

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 1009

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1010

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:

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 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.

 Licensed to Berend Post berend.post@it-university.nl

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.

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.

Licensed to Berend Post berend.post@it-university.nl

Reference:

CISA review manual 2014 Page number 166

Question 1011

During the planning stage of a compliance audit, an IS auditor discovers that a bank's inventory of compliance requirements does not include recent regulatory changes related to managing data risk. What should the auditor do FIRST?

- ☐ Discuss potential regulatory issues with the legal department.
- ☒ Ask management why the regulatory changes have not been included.
- ☐ Exclude recent regulatory changes from the audit scope.
- ☐ Report the missing regulatory updates to the chief information officer (CIO).

Question 1012

Which of the following approaches would utilize data analytics to facilitate the testing of a new account creation process?

- ☒ Review the business requirements document for date of birth field requirements.
- ☐ Review new account applications submitted in the past month for invalid dates of birth.
- ☐ Evaluate configuration settings for the date of birth field requirements.
- ☐ Attempt to submit new account applications with invalid dates of birth.

Question 1013

When facilitating the alignment of corporate governance and information security governance, which of the following is the MOST important role of an organization's security steering committee?

- ☐ Obtaining support for the integration from business owners
- ☐ Obtaining approval for the information security budget
- ☒ Evaluating and reporting the degree of integration
- ☐ Defining metrics to demonstrate alignment

Question 1014

Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

- ☐ Intrusion detection systems
- ☒ Data mining techniques
- ☐ Firewalls
- ☐ Packet filtering routers

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Data mining is a technique used to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

Question 1015

Which of the following BEST demonstrates to an IS auditor that an organization has implemented effective risk management processes?

- ☐ Critical business assets have additional controls.
- ☐ The risk register is reviewed periodically.
- ☐ A business impact analysis (BIA) has been completed.
- ☒ The inventory of IT assets includes asset classification.

Question 1016

An IS auditor evaluating logical access controls should FIRST:

- ☐ document the controls applied to the potential access paths to the system.
- ☐ test controls over the access paths to determine if they are functional.
- ☐ evaluate the security environment in relation to written policies and practices
- ☒ obtain an understanding of the security risks to information processing.

Explanation:

Explanation:

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths-to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

Question 1017

Which of the following is the PRIMARY reason for an IS auditor to map out the narrative of a business process?

- ☐ To verify the business process is as described in the engagement letter
- ☒ To identify the resources required to perform the audit
- ☐ To ensure alignment with organizational objectives
- ☐ To gain insight into potential risks

Licensed to Berend Post berend.post@it-university.nl

Question 1018

Which of the following is the BEST way for an IS auditor to assess the effectiveness of backup procedures?

- ☐ Review the backup schedule.
- ☐ Evaluate the latest data restore.
- ☒ Inspect backup logs.
- ☐ Interview the data owner.

Question 1019

An IS auditor finds the log management system is overwhelmed with false positive alerts. The auditor's BEST recommendation would be to:

- ☐ recruit more monitoring personnel.
- ☐ fine tune the intrusion detection system (IDS).
- ☐ reduce the firewall rules.
- ☒ establish criteria for reviewing alerts.

Question 1020

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 1021

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

Licensed to Berend Post berend.post@it-university.nl

and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics.

Additionally, less importance is placed on formal paper- based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of greater importance.

Question 1022

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.

Question 1023

Which of the following would provide management with the MOST reasonable assurance that a new data warehouse will meet the needs of the organization?

- ☒ Appointing data stewards to provide effective data governance
- ☐ Classifying data quality issues by the severity of their impact to the organization
- ☐ Integrating data requirements into the system development life cycle (SDLC)
- ☐ Facilitating effective communication between management and developers

Licensed to Berend Post berend.post@it-university.nl

Question 1024

When conducting a follow-up audit on an organization's firewall configuration, the IS auditor discovered that the firewall had been integrated into a new system that provides both firewall and intrusion detection capabilities. The IS auditor should:

- ☐ consider the follow-up audit unnecessary since the firewall is no longer being used.
- ☒ assess whether the integrated system addresses the identified risk.
- ☐ review the compatibility of the new system with existing network controls.
- ☐ evaluate whether current staff is able to support the new system.

Question 1025

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 1026

Which of the following is BEST for providing uninterrupted services?

- ☐ Snapshots
- ☐ Differential backup
- ☐ Televaulting
- ☒ Mirroring

Licensed to Berend Post berend.post@it-university.nl

Question 1027

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 1028

Which of the following is the BEST detective control for a job scheduling process involving data transmission?

☐ Metrics denoting the volume of monthly job failures are reported and reviewed by senior management.
☒ Job failure alerts are automatically generated and routed to support personnel.
☐ Jobs are scheduled and a log of this activity is retained for subsequent review.
☐ Jobs are scheduled to be completed daily and data is transmitted using a secure File Transfer Protocol (FTP).

Question 1029

To protect information assets, which of the following should be done FIRST?

☐ Restrict access to data
☐ Encrypt data
☒ Classify data
☐ Back up data

Question 1030

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

Licensed to Berend Post berend.post@it-university.nl

an application system and processing test or production data against the entity as a means of verifying processing accuracy.

Question 1031

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 1032

Which of the following provides an IS auditor the MOST assurance that an organization is compliant with legal and regulatory requirements?

- ☐ The IT manager is responsible for the organization's compliance with legal and regulatory requirements.
- ☒ Controls associated with legal and regulatory requirements have been identified and tested.
- ☐ Senior management has provided attestation of legal and regulatory compliance.
- ☐ There is no history of complaints or fines from regulators regarding noncompliance.

Question 1033

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 1034

A live test of a mutual agreement for IT system recovery has been carried out, including a four- hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

- ☒ system and the IT operations team can sustain operations in the emergency environment.
- ☐ resources and the environment could sustain the transaction load.
- ☐ connectivity to the applications at the remote site meets response time requirements.
- ☐ workflow of actual business operations can use the emergency system in case of a disaster.

Explanation:

Explanation:

The applications have been intensively operated, therefore choices B, C and D have been actually tested, but the capability of the system and the IT operations team to sustain and support this environment (ancillary operations, batch closing, error corrections, output distribution, etc.) is only partially tested.

Question 1035

An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

- ☒ a data loss of up to 1 minute, but the processing must be continuous.
- ☐ a 1-minute processing interruption but cannot tolerate any data loss.
- ☐ a processing interruption of 1 minute or more.
- ☐ both a data less and processing interruption longer than 1 minute.

Explanation:

Explanation:

The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

Licensed to Berend Post berend.post@it-university.nl

Question 1036

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 1037

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 1038

Which of the following message services provides the strongest evidence that a specific action has occurred?

- ☐ Proof of delivery
- ☒ Nonrepudiation
- ☐ Proof of submission
- ☐ Message origin authentication

Explanation:

Explanation:

Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts, i.e., proof of submission, proof of delivery and

Licensed to Berend Post berend.post@it-university.nl

message origin authentication. However, nonrepudiation provides stronger evidence because the proof can be demonstrated to a third party. Digital signatures are used to provide nonrepudiation. Message origination authentication will only confirm the source of the message and does not confirm the specification that has been completed.

Question 1039

Which of the following BEST limits the impact of server failures in a distributed environment?

- ☐ Redundant pathways
- ☒ Clustering
- ☐ Dial backup lines
- ☐ Standby power

Explanation:

Explanation:

Clustering allows two or more servers to work as a unit, so that when one of them fails, the other takes over. Choices A and C are intended to minimize the impact of channel communications failures, but not a server failure. Choice D provides an alternative power source in the event of an energy failure.

Question 1040

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 1041

Which of the following is the BEST method to assess the adequacy of security awareness in an organization?

- ☐ Confirming a security awareness program exists
- ☐ Interviewing employees about security responsibility
- ☒ Administering security survey questionnaires
- ☐ Observing employee security behaviors

Licensed to Berend Post berend.post@it-university.nl

Question 1042

Which of the following should be of MOST influence to an information security manager when developing IT security policies?

- ☐ Past and current threats
- ☐ IT security framework
- ☐ Compliance with regulations
- ☒ Business strategy

Question 1043

The business case for an IS project has changed during the course of the project due to new requirements being added. What should be done NEXT?

- ☐ The project should go through the formal reapproval process.
- ☐ The changes to the business case should be documented in the project plan.
- ☐ Additional resources should be allocated to the project due to the new requirements.
- ☒ Project stakeholders should be notified of the changes.

Question 1044

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1045

To integrate security into system development life cycle (SDLC) processes, an organization MUST ensure that security:

- ☒ is a prerequisite for completion of major phases.
- ☐ performance metrics have been met.
- ☐ roles and responsibilities have been defined.
- ☐ is represented on the configuration control board.

Question 1046

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

- ☐ Personally delete all copies of the unauthorized software.
- ☐ Inform the auditee of the unauthorized software, and follow up to confirm deletion.
- ☒ Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
- ☐ Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Explanation:

Explanation:

The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

Question 1047

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

Licensed to Berend Post berend.post@it-university.nl

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 1048

Which of the following is the BEST defense against a brute force attack?

- ☐ Discretionary access control
- ☐ Intruder detection lockout
- ☐ Mandatory access control
- ☒ Time-of-day restrictions

Question 1049

Which of the following is the BEST way for an IT forensics investigator to detect evidence of steganography?

- ☒ Compare file hashes between original and modified image files.
- ☐ Identify and analyze emergent properties within a file system's metadata.
- ☐ Recover deleted files from a suspected hard drive utilizing forensics software.
- ☐ Scan computer operating systems using administrative tools.

Question 1050

During a software acquisition review, an IS auditor should recommend that there be a software escrow agreement when:

- ☐ the estimated life for the product is less than 3 years.
- ☒ the deliverables do not include the source code.
- ☐ the product is new in the market.
- ☐ there is no service level agreement (SLA).

Licensed to Berend Post berend.post@it-university.nl

Question 1051

The effectiveness of an incident response team will be GREATEST when:

- ☒ the incident response process is updated based on lessons learned
- ☐ incidents are identified using a security information and event monitoring (SIEM) system
- ☐ the incident response team members are trained security personnel
- ☐ the incident response team meets on a regular basis to review log files

Question 1052

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:

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:

Licensed to Berend Post berend.post@it-university.nl

A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key

A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requester

A Subscriber is the end user who wish to get digital certificate from certificate authority.

The following were incorrect answers:

The Certificate authority role is to issue digital certificates to end users - This is a valid statement as the job of a certificate authority is to issue a digital certificate to end user.

The Registration authority (RA) acts as a verifier for Certificate Authority (CA) - This is a valid statement as registration authority acts as a verifier for certificate authority

Root certificate authority's certificate is always self-signed - This is a valid statement as the root certificate authority's certificate is always self-signed.

Reference:

http://searchsecurity.techtarget.com/definition/PKI

Question 1053

In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- ☒ Nonrepudiation
- ☐ Encryption
- ☐ Authentication
- ☐ Integrity

Explanation:

Explanation:

Nonrepudiation, achieved through the use of digital signatures, prevents the claimed sender from later denying that they generated and sent the message. Encryption may protect the data transmitted over the Internet, but may not prove that the transactions were made. Authentication is necessary to establish the identification of all parties to a communication. Integrity ensures that transactions are accurate but does not provide the identification of the customer.

Licensed to Berend Post berend.post@it-university.nl

Question 1054

An organization is concerned about duplicate vendor payments on a complex system with a high volume of transactions. Which of the following would be MOST helpful to an IS auditor to determine whether duplicate vendor payments exist?

- ☒ Computer-assisted technique
- ☐ Stop-and-go testing
- ☐ Statistical sampling
- ☐ Judgmental sampling

Question 1055

Planning for the implementation of an information security program is MOST effective when it:

- ☐ uses risk-based analysis for security projects.
- ☐ applies technology-driven solutions to identified needs.
- ☐ uses decision trees to prioritize security projects.
- ☒ applies gap analysis to current and future business plans.

Question 1056

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1057

Which of the following would the IS auditor MOST likely review to determine whether modifications to the operating system parameters were authorized?

- ☒ Change control log
- ☐ System initialization logs
- ☐ Security system parameters
- ☐ Documentation of exit routines

Question 1058

Which of the following is MOST important for the improvement of an organization's incident response processes?

- ☒ Post-event reviews by the incident response team
- ☐ Regular upgrades to incident management software
- ☐ Ongoing incident response training for users
- ☐ Periodic walk-through of incident response procedures

Question 1059

Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

- ☐ System log analysis
- ☒ Compliance testing
- ☐ Forensic analysis
- ☐ Analytical review

Explanation:

Explanation:

Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs. Forensic analysis is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

Licensed to Berend Post berend.post@it-university.nl

Question 1060

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 1061

The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

- ☒ integrity.
- ☐ authenticity.
- ☐ authorization.
- ☐ nonrepudiation.

Explanation:

Explanation:

A checksum calculated on an amount field and included in the EDI communication can be used to identify unauthorized modifications. Authenticity and authorization cannot be established by a checksum alone and need other controls. Nonrepudiation can be ensured by using digital signatures.

Question 1062

Which of the following is the GREATEST concern when an organization's disaster recovery strategy utilizes a cold site?

- ☐ The lack of electrical power connections
- ☐ The lack of networking infrastructure
- ☐ The lack of appropriate environmental controls
- ☒ The lack of hardware components availability

Licensed to Berend Post berend.post@it-university.nl

Question 1063

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?

- ☐ CRC-32
- ☐ CRC-64
- ☐ DES
- ☐ 3DES
- ☒ RC4
- ☐ RC5
- ☐ None of the choices.

Explanation:

Explanation:

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity.

Question 1064

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

- ☒ symmetric encryption.
- ☐ message authentication code.
- ☐ hash function.
- ☐ digital signature certificates.

Explanation:

Explanation:

SSL uses a symmetric key for message encryption. A message authentication code is used for ensuring data integrity. Hash function is used for generating a message digest; it does not use public key encryption for message encryption. Digital signature certificates are used by SSL for server authentication.

Question 1065

What is the most common reason for information systems to fail to meet the needs of users?

- ☐ Lack of funding
- ☒ Inadequate user participation during system requirements definition
- ☐ Inadequate senior management participation during system requirements definition
- ☐ Poor IT strategic planning

Explanation:

Explanation:

Inadequate user participation during system requirements definition is the most common reason for information systems to fail to meet the needs of users.

Licensed to Berend Post berend.post@it-university.nl

Question 1066

In the event of a data center disaster, which of the following would be the MOST appropriate strategy to enable a complete recovery of a critical database?

- ☐ Daily data backup to tape and storage at a remote site
- ☒ Real-time replication to a remote site
- ☐ Hard disk mirroring to a local server
- ☐ Real-time data backup to the local storage area network (SAN)

Explanation:

Explanation:

With real-time replication to a remote site, data are updated simultaneously in two separate locations; therefore, a disaster in one site would not damage the information located in the remote site. This assumes that both sites were not affected by the disaster. Daily tape backup recovery could lose up to a day's work of data. Choices C and D take place in the same data center and could possibly be affected by the same disaster.

Question 1067

When protecting the confidentiality of information assets, the MOST effective control practice is the:

- ☐ awareness training of personnel on regulatory requirements.
- ☐ enforcement of a need-to-know access control philosophy.
- ☒ utilization of a dual-factor authentication mechanism.
- ☐ configuration of read-only access to all users.

Question 1068

A core business unit relies on an effective legacy system that does not meet the current security standards and threatens the enterprise network. Which of the following is the BESTcourse of action to address the situation?

- ☐ Require that new systems that can meet the standards be implemented.
- ☐ Document the deficiencies in the risk register.
- ☒ Develop processes to compensate for the deficiencies.
- ☐ Disconnect the legacy system from the rest of the network.

Licensed to Berend Post berend.post@it-university.nl

Question 1069

Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

- ☐ System analysis
- ☒ Authorization of access to data
- ☐ Application programming
- ☐ Data administration

Explanation:

Explanation:

The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

Question 1070

What should an IS auditor do when informed that some recommendations cannot be implemented due to financial constraints?

- ☒ Document management's response in the working papers.
- ☐ Insist the recommendations be implemented.
- ☐ Agree to waive the recommendations.
- ☐ Suggest management identify cost-effective alternatives.

Question 1071

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1072

Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called a:

- ☐ feedback error control.
- ☐ block sum check.
- ☒ forward error control.
- ☐ cyclic redundancy check.

Explanation:

Explanation:

Forward error control involves transmitting additional redundant information with each character or frame to facilitate detection and correction of errors, in feedback error control, only enough additional information is transmitted so the receiver can identify that an error has occurred.

Choices B and D are both error detection methods but not error correction methods. Block sum check is an extension of parity check wherein an additional set of parity bits is computed for a block of characters. A cyclic redundancy check is a technique wherein a single set of check digits is generated, based on the contents of the frame, for each frame transmitted.

Question 1073

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 1074

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)

Licensed to Berend Post berend.post@it-university.nl

Question 1075

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 1076

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 1077

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 1078

Minimum password length and password complexity verification are examples of:

- ☐ detection controls.
- ☐ control objectives.
- ☐ audit objectives.
- ☒ control procedures.

Explanation:

Explanation:

Control procedures are practices established by management to achieve specific control objectives. Password controls are preventive controls, not detective controls. Control objectives are declarations of expected results from implementing controls and audit objectives are the specific goals of an audit.

Question 1079

A vendor service level agreement (SLA) requires backups to be physically secured. An IS audit of the backup system revealed a number of the backup media were missing. Which of the following should be the auditor's NEXT step?

- ☐ Recommend a review of the vendor's contract.
- ☒ Recommend identification of the data stored on the missing media.
- ☐ Notify executive management.
- ☐ Include the missing backup media finding in the audit report.

Licensed to Berend Post berend.post@it-university.nl

Question 1080

Which of the following is the BEST indication of control maturity in an organization's systems development and implementation processes?

- ☐ Code changes are tested and deployed manually.
- ☐ Code changes are deployed to a test server and then to production.
- ☐ Code changes are documented and approved.
- ☒ Code changes are tested and deployed through automation.

Question 1081

An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

- ☐ report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
- ☐ verify that user access rights have been granted on a need-to-have basis.
- ☒ recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
- ☐ recommend that activity logs of terminated users be reviewed on a regular basis.

Explanation:

Explanation:

Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate, the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted.

Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

Question 1082

An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

- ☐ alignment of the BCP with industry best practices.
- ☒ results of business continuity tests performed by IS and end-user personnel.
- ☐ off-site facility, its contents, security and environmental controls.
- ☐ annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

Question 1083

Which of the following would BEST detect that a distributed-denial-of-service attack (DDoS) is occurring?

- ☐ Server crashes
- ☒ Automated monitoring of logs
- ☐ Penetration testing
- ☐ Customer service complaints

Question 1084

Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource?

- ☐ Systems logs
- ☒ Access control lists (ACL)
- ☐ Application logs
- ☐ Error logs

Explanation:

Explanation:

IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

Question 1085

An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would BEST mitigate the risk of undetected and unauthorized program changes to the production environment?

- ☐ Commands typed on the command line are logged
- ☒ Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs
- ☐ Access to the operating system command line is granted through an access restriction tool with preapproved rights
- ☐ Software development tools and compilers have been removed from the production environment

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The matching of hash keys over time would allow detection of changes to files. Choice A is incorrect because having a log is not a control, reviewing the log is a control. Choice C is incorrect because the access was already granted-it does not matter how. Choice D is wrong because files can be copied to and from the production environment.

Question 1086

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

Question 1087

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:

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

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

Licensed to Berend Post berend.post@it-university.nl

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

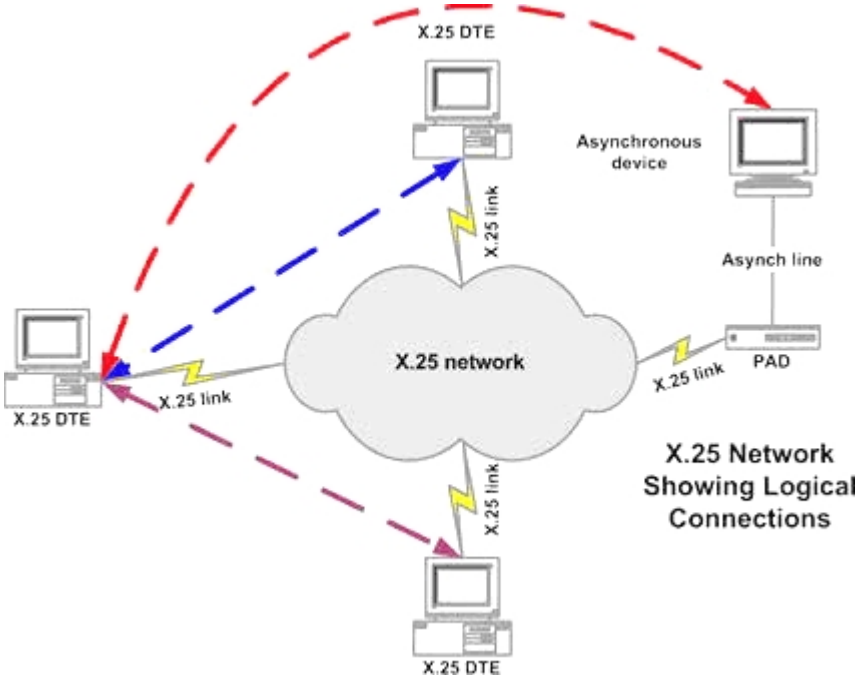
X.25

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

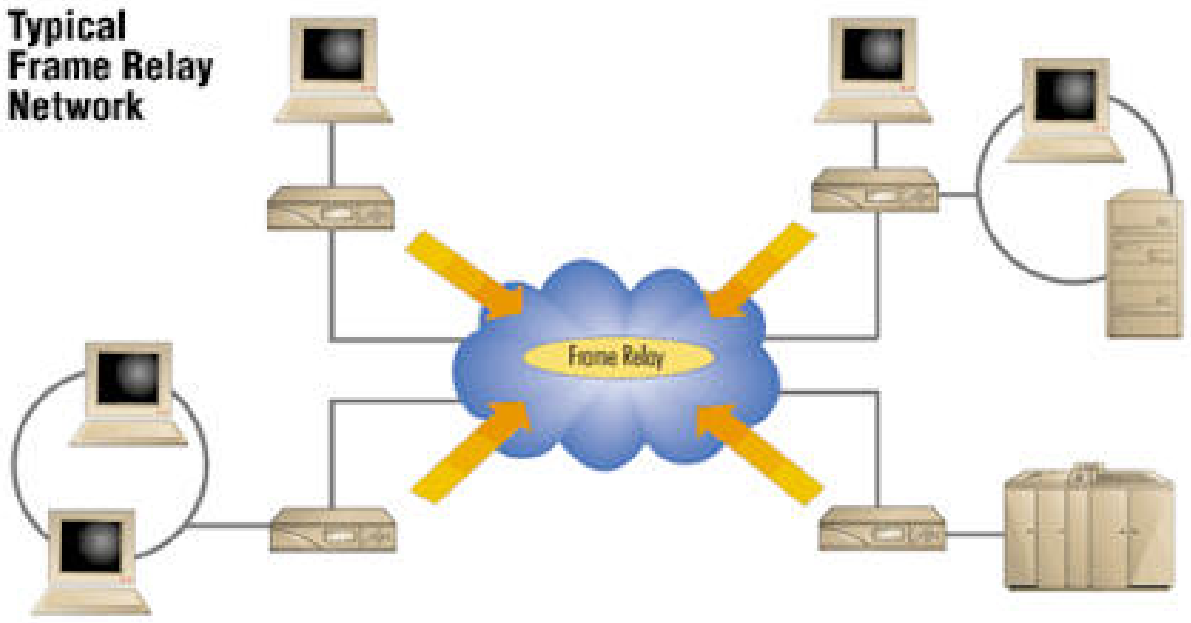
Companies that pay more to ensure that a higher level of bandwidth will always be available, pay a committed information rate or CIR

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.



Frame Relay

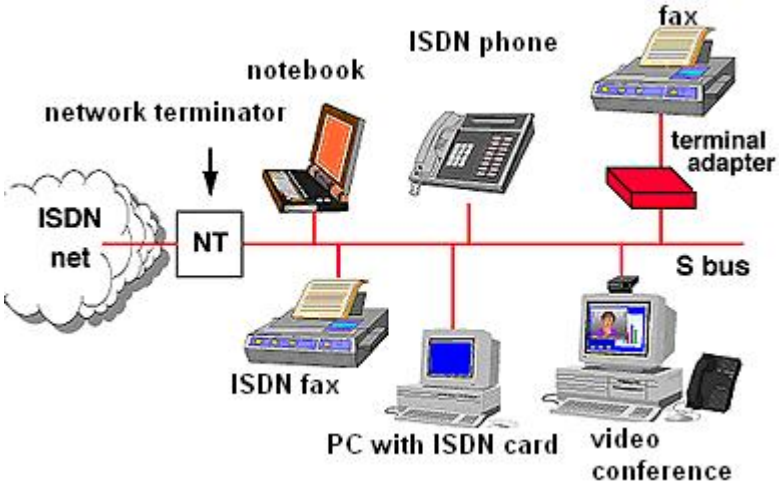
Licensed to Berend Post berend.post@it-university.nl

Integrated Service Digital Network

Enables data, voice and other types of traffic to travel over a medium in a digital manner previously used only for analog voice transmission.

Same copper telephone wire is used.

Provide digital point-to-point circuit switching medium.



ISDN

Asynchronous Transfer Mode (ATM)

Uses Cell switching method

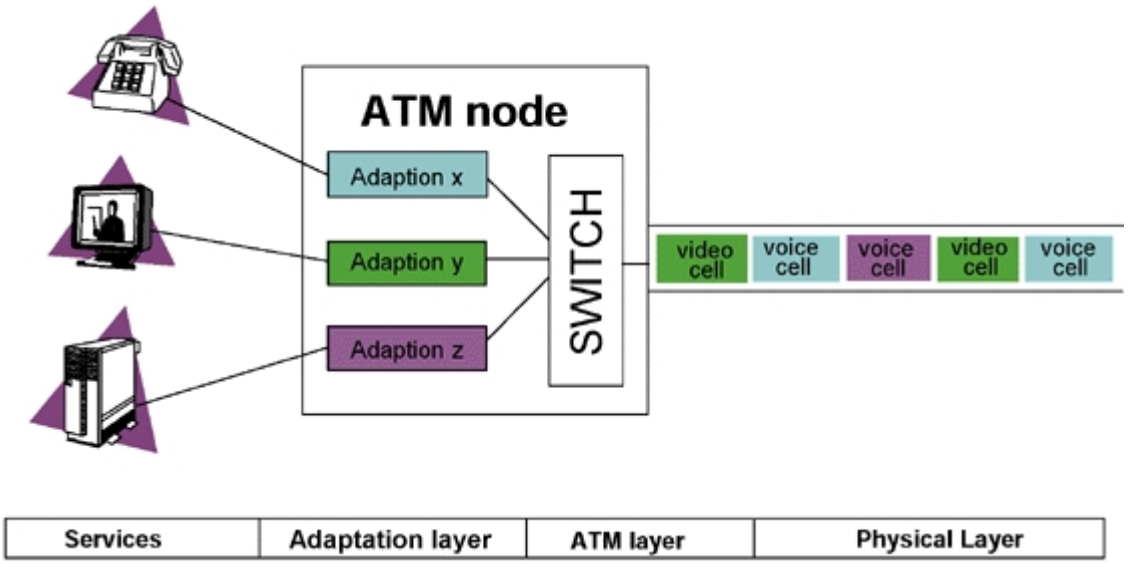
High speed network technology used for LAN, MAN and WAN

Like a frame relay it is connection oriented technology which creates and uses fixed channel

Data are segmented into fixed size cell of 53 bytes

Some companies have replaces FDDI back-end with ATM

Licensed to Berend Post berend.post@it-university.nl



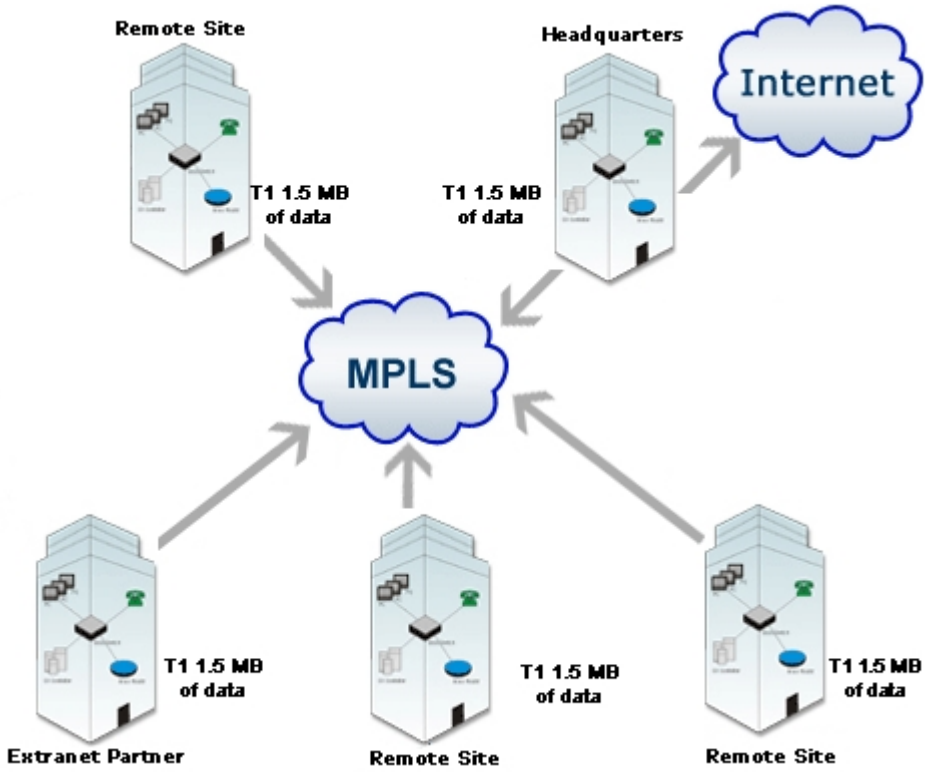
Asynchronous Transfer Mode

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.

Reference:

CISA review manual 2014 page number 266

Question 1088

When conducting a post-incident review, the GREATEST benefit of collecting mean time to resolution (MTTR) data is the ability to:

- ☐ reduce the costs of future preventive controls
- ☐ provide metrics for reporting to senior management
- ☐ verify compliance with the service level agreement (SLA)
- ☒ learn of potential areas of improvement

Licensed to Berend Post berend.post@it-university.nl

Question 1089

During the course of an audit, an IS auditor's organizational independence is impaired. The IS auditor should FIRST:

- ☒ inform audit management of the situation.
- ☐ inform senior management in writing and proceed with the audit.
- ☐ obtain the auditee's approval before continuing the audit.
- ☐ proceed with the audit as planned after documenting the incident.

Question 1090

An IS auditor finds that a company is using a payroll provider hosted in a foreign country. Of the following, the MOST important audit consideration is whether the provider's operations:

- ☐ meet industry best practice and standards
- ☒ comply with applicable laws and regulations
- ☐ are shared with other companies using the provider
- ☐ are aligned with the company's culture

Question 1091

Which of the following requires a consensus by key stakeholders on IT strategic goals and objectives?

- ☒ Balanced scorecards
- ☐ Benchmarking
- ☐ Maturity models
- ☐ Peer reviews

Question 1092

Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

- ☐ Invite client participation.
- ☐ involve all technical staff.
- ☒ Rotate recovery managers.
- ☐ install locally-stored backup.

Explanation:

Explanation:

Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

Licensed to Berend Post berend.post@it-university.nl

Question 1093

Which of the following dynamic interaction of a Business Model for Information Security (BMIS) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management?

- ☐ Governing
- ☐ Culture
- ☐ Enabling and support
- ☒ Emergence

Explanation:

Explanation:

Emergence – which connotes surfacing, developing, growing and evolving – refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control. The emergence dynamic interconnection (between people and processes) is a place to introduce possible solutions such as feedback loops; alignment with process improvement; and consideration of emergent issues in system design life cycle, change control, and risk management.

For your exam you should know the information below.

Business Model for Information Security

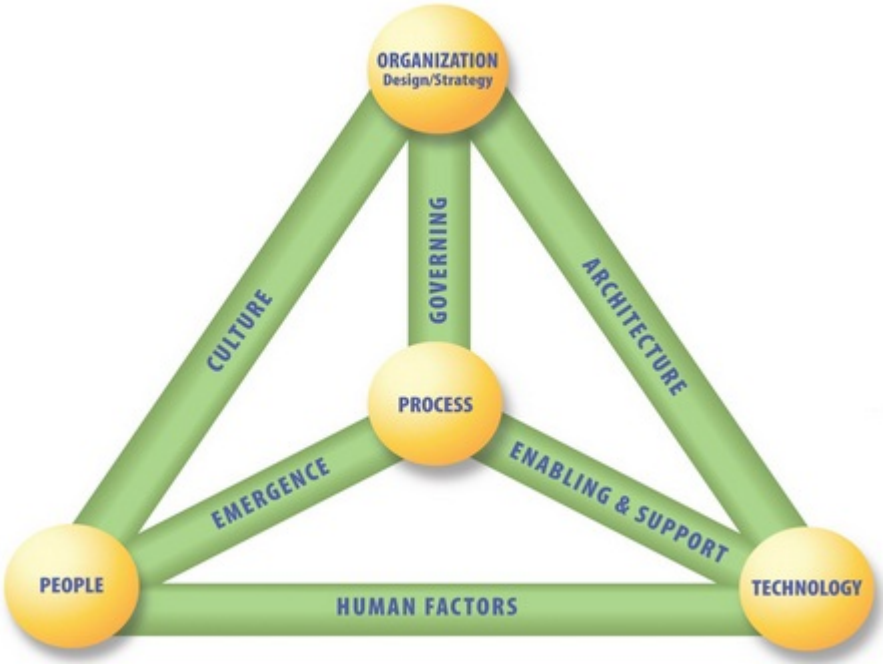
The Business Model for Information Security (BMIS) originated at the Institute for Critical Information Infrastructure Protection at the Marshall School of Business at the University of Southern California in the USA. ISACA has undertaken the development of the Systemic Security Management Model. The 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

Licensed to Berend Post berend.post@it-university.nl

management of any discipline within the enterprise can be enhanced by approaching it from a systems thinking perspective, its implementation will certainly help with managing risk.

The success that the systems approach has achieved in other fields bodes well for the benefits it can bring to security. The often dramatic failures of enterprises to adequately address security issues in recent years are due, to a significant extent, to their inability to define security and present it in a way that is comprehensible and relevant to all stakeholders. Utilizing a systems approach to information security management will help information security managers address complex and dynamic environments, and will generate a beneficial effect on collaboration within the enterprise, adaptation to operational change, navigation of strategic uncertainty and tolerance of the impact of external factors. The model is represented below.



As illustrated in above, the model is best viewed as a flexible, three-dimensional, pyramid-shaped structure made up of four elements linked together by six dynamic interconnections.

All aspects of the model interact with each other. If any one part of the model is changed, not addressed or managed inappropriately, the equilibrium of the model is potentially at risk. The dynamic interconnections act as tensions, exerting a push/pull force in reaction to changes in the enterprise, allowing the model to adapt as needed.

The four elements of the model are:

Licensed to Berend Post berend.post@it-university.nl

1. Organization Design and Strategy – organization is a network of people, assets and processes interacting with each other in defined roles and working toward a common goal.

An enterprise's strategy specifies its business goals and the objectives to be achieved as well as the values and missions to be pursued. It is the enterprise's formula for success and sets its basic direction. The strategy should adapt to external and internal factors. Resources are the primary material to design the strategy and can be of different types (people, equipment, know-how). Design defines how the organization implements its strategy. Processes, culture and architecture are important in determining the design.

2. People – The human resources and the security issues that surround them. It defines who implements (through design) each part of the strategy. It represents a human collective and must take into account values, behaviors and biases. Internally, it is critical for the information security manager to work with the human resources and legal departments to address issues such as:

Recruitment strategies (access, background checks, interviews, roles and responsibilities)

Employment issues (location of office, access to tools and data, training and awareness, movement within the enterprise)

Termination (reasons for leaving, timing of exit, roles and responsibilities, access to systems, access to other employees). Externally, customers, suppliers, media, stakeholders and others can have a strong influence on the enterprise and need to be considered within the security posture.

3. Process – Includes formal and informal mechanisms (large and small, simple and complex) to get things done and provides a vital link to all of the dynamic interconnections.

Processes identify, measure, manage and control risk, availability, integrity and confidentiality, and they also ensure accountability. They derive from the strategy and implement the operational part of the organization element.

To be advantageous to the enterprise, processes must:

Meet business requirements and align with policy

Consider emergence and be adaptable to changing requirements

Be well documented and communicated to appropriate human resources

Be reviewed periodically, once they are in place, to ensure efficiency and effectiveness

4. Technology – Composed of all of the tools, applications and infrastructure that make processes more efficient. As an evolving element that experiences frequent changes, it has its own dynamic risk. Given the typical enterprise's dependence on technology, technology constitutes a core part of the enterprise's infrastructure and a critical component in accomplishing its mission.

Technology is often seen by the enterprise's management team as a way to resolve security threats and risk. While technical controls are helpful in mitigating some types of risk, technology should not be viewed as an information security solution.

Licensed to Berend Post berend.post@it-university.nl

Technology is greatly impacted by users and by organizational culture. Some individuals still mistrust technology; some have not learned to use it; and others feel it slows them down. Regardless of the reason, information security managers must be aware that many people will try to sidestep technical controls.

Dynamic Interconnections

The dynamic interconnections are what link the elements together and exert a multidirectional force that pushes and pulls as things change. Actions and behaviors that occur in the dynamic interconnections can force the model out of balance or bring it back to equilibrium.

The six dynamic interconnections are:

1. Governing – Governing is the steering of the enterprise and demands strategic leadership. Governing sets limits within which an enterprise operates and is implemented within processes to monitor performance, describe activities and achieve compliance while also providing adaptability to emergent conditions. Governing incorporates ensuring that objectives are determined and defined, ascertaining that risks are managed appropriately, and verifying that the enterprise's resources are used responsibly.

2. Culture – Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things. It is emergent and learned, and it creates a sense of comfort. Culture evolves as a type of shared history as a group goes through a set of common experiences. Those similar experiences cause certain responses, which become a set of expected and shared behaviors. These behaviors become unwritten rules, which become norms that are shared by all people who have that common history. It is important to understand the culture of the enterprise because it profoundly influences what information is considered, how it is interpreted and what will be done with it. Culture may exist on many levels, such as national (legislation/regulation, political and traditional), organizational (policies, hierarchical style and expectations) and social (family, etiquette). It is created from both external and internal factors, and is influenced by and influences organizational patterns.

3. Enabling and support – The enabling and support dynamic interconnection connects the technology element to the process element. One way to help ensure that people comply with technical security measures, policies and procedures is to make processes usable and easy. Transparency can help generate acceptance for security controls by assuring users that security will not inhibit their ability to work effectively. Many of the actions that affect both technology and processes occur in the enabling and support dynamic interconnection. Policies, standards and guidelines must be designed to support the needs of the business by reducing or eliminating conflicts of interest, remaining flexible to support changing business objectives, and being acceptable and easy for people to follow.

Licensed to Berend Post berend.post@it-university.nl

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.

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.

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

CISA review manual 2014 page number 37 and 38

http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf

Question 1094

Meeting which of the following security objectives BEST ensures that information is protected against unauthorized modification?

- ☐ Availability
- ☐ Authenticity
- ☐ Confidentiality
- ☒ Integrity

Question 1095

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1096

Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

- ☐ all threats can be completely removed.
- ☒ a cost-effective, built-in resilience can be implemented.
- ☐ the recovery time objective can be optimized.
- ☐ the cost of recovery can be minimized.

Explanation:

Explanation:

It is critical to initially identify information assets that can be made more resilient to disasters, e.g., diverse routing, alternate paths or multiple communication carriers. It is impossible to remove all existing and future threats. The optimization of the recovery time objective and efforts to minimize the cost of recovery come later in the development of the disaster recovery strategy.

Question 1097

Which of the following PBX feature allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available?

- ☒ Automatic Call distribution
- ☐ Call forwarding
- ☐ Tenanting
- ☐ Voice mail

Explanation:

Explanation:

Automatic Call distribution allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

For your exam you should know below mentioned PBX features and Risks:

System Features

Description

Risk

Automatic Call distribution

Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available

Licensed to Berend Post berend.post@it-university.nl

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

Eavesdropping, by adding unwanted/unknown parties to a conference

override(intrude)

Licensed to Berend Post berend.post@it-university.nl

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

Allows calls to an in-use extension to be added to a conference when that extension is on conference and already off-hook

Licensed to Berend Post berend.post@it-university.nl

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:

Call forwarding - Allow specifying an alternate number to which calls will be forwarded based on certain condition

Tenanting - Limits system user access to only those users who belong to the same tenant group useful when one company leases out part of its building to other companies and tenants share an attendant, trunk lines,etc

Voice Mail - Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.

Reference:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 Page number 358

Question 1098

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.

Question 1099

Which of the following roles should be PRIMARILY responsible for assigning sensitivity levels to an organization's financial and payroll databases?

- ☐ Information security manager
- ☒ Data owner
- ☐ Systems administrator
- ☐ Database administrator

Question 1100

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- ☐ Security incident summaries
- ☐ Vendor best practices
- ☐ CERT coordination center
- ☒ Significant contracts

Explanation:

Explanation:

Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets. Vendor best practices provides a basis for

Licensed to Berend Post berend.post@it-university.nl

evaluating how competitive an enterprise is, while security incident summaries are a source for assessing the vulnerabilities associated with the IT infrastructure. CERT (www.cert.org) is an information source for assessing vulnerabilities within the IT infrastructure.

Question 1101

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 1102

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 1103

An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

- ☐ The new access points with stronger security are affordable.
- ☐ The old access points are poorer in terms of performance.
- ☒ The organization's security would be as strong as its weakest points.
- ☐ The new access points are easier to manage.

Explanation:

Explanation:

The old access points should be discarded and replaced with products having strong security; otherwise, they will leave security holes open for attackers and thus make the entire network as weak as they are. Affordability is not the auditor's major concern. Performance is not as important as security in this situation. Product manageability is not the IS auditor's concern.

Licensed to Berend Post berend.post@it-university.nl

Question 1104

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 1105

To gain a clear understanding of the impact that a new regulatory requirement will have on an organization's information security controls, an information security manager should FIRST:

- ☐ conduct a risk assessment.
- ☒ perform a gap analysis.
- ☐ conduct a cost-benefit analysis.
- ☐ interview senior management.

Question 1106

Which of the following would be the PRIMARY benefit of replacing physical keys with an electronic badge system for access to a data center?

- ☒ Increasing accountability
- ☐ Maintaining compliance
- ☐ Tracking employee work hours
- ☐ Increasing reliability

Question 1107

Which of the following is a MAJOR benefit of using a wireless network?

- ☐ Faster network speed
- ☒ Stronger authentication
- ☐ Protection against eavesdropping
- ☐ Lower installation cost

Licensed to Berend Post berend.post@it-university.nl

Question 1108

An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

- ☒ Network workstations are not disabled automatically after a period of inactivity.
- ☐ Wiring closets are left unlocked
- ☐ Network operating manuals and documentation are not properly secured.
- ☐ Network components are not equipped with an uninterruptible power supply.

Explanation:

Explanation:

Choice A is the only logical security finding. Network logical security controls should be in place to restrict, identify, and report authorized and unauthorized users of the network. Disabling inactive workstations restricts users of the network. Choice D is an environmental issue and choices B and C are physical security issues. Choices B, C and D should be reported to the appropriate entity.

Question 1109

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 1110

Which of the following is the BEST indicator of a mature quality management system (QMS)?

- ☐ Projects are showing continuous improvement.
- ☐ Continuous improvement has been integrated into business processes.
- ☐ End users are satisfied with the outcome of IT projects.
- ☒ Most IT projects have been completed on time and within budget.

Licensed to Berend Post berend.post@it-university.nl

Question 1111

Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

- ☒ The alternate facility will be available until the original information processing facility is restored.
- ☐ User management is involved in the identification of critical systems and their associated critical recovery times.
- ☐ Copies of the plan are kept at the homes of key decision-making personnel.
- ☐ Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Explanation:

Explanation:

The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or the execution pf the plan.

Question 1112

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 1113

Which of the following function in traditional EDI translate data between the standard format and trading partner's propriety format?

- ☐ Communication handler
- ☐ Application Interface
- ☐ Application System
- ☒ EDI Translator

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

EDI Translator translates data between standard format (ANSI X12) and trading partner's propriety information.

For CISA Exam you should know below information about Traditional EDI functions.

Moving data in a batch transmission process through the traditional EDI process generally involves three functions within each trading partner's computer system

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN). VAN use computerized message switching and storage capabilities to provide electronic mailbox services similar to post offices. The VAN receives all the outbound transactions from an organization, sort them by destination and passes them to precipitants when they log on to check their mailbox and receive transmission.

EDI Interface – Interface function that manipulates and routes data between the application system and the communication handler. The interface consists of two components

EDI Translator – The device translates data between standard format (ANSI X12) and trading partner's propriety information.

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping. Data mapping is the process by which data are extracted from EDI translation process and integrated with the data or process of receiving company.

3. Application System – The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

The following were incorrect answers:

Communication handler – Process for transmitting and receiving electronic documents between trading partners via dial-up lines, public switched networks, multiple dedicated lines or a value added network (VAN).

Licensed to Berend Post berend.post@it-university.nl

Application System – The program that process the data sent to, or received from, the trading partner. Although new controls should be developed for the EDI interface, the control for existing applications, if left unchanged, are usually unaffected.

Application Interface – This interface moves electronic transactions to or from the application systems and perform data mapping.

Reference:

CISA review manual 2014 Page number 178

Question 1114

As an IS auditor it is very important to understand software release management process. Which of the following software release normally contains small enhancements and fixes?

- ☐ Major software Release
- ☒ Minor software Release
- ☐ Emergency software release
- ☐ General software Release

Explanation:

Explanation:

Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

For CISA exam you should know below information about software release management:

Software Release Management is the process of ensuring releases can be reliably planned, scheduled and successfully transitioned (deployed) to Test and Live Environments. Software Release Management is not just about "automating the path to production" although that is certainly an important part. It also about adopting a holistic view of application changes, using the "Release" as the container to ensure that changes are packaged, released and tested in a repeatable and controlled manner. Release Management is often likened to the conductor of an orchestra, with the individual changes to be implemented the various instruments within it. Software Release Management is intrinsically linked with the more well understood and adopted Software Change and Configuration Management disciplines.

Licensed to Berend Post berend.post@it-university.nl

Software Release management is a process through which software is made available to user. Each update or upgrade of a Configuration Item is referred to as a release.

There are three levels of releases. These levels related to releasing hardware or software into your IT infrastructure. Some may be a single change, others may implement many changes at a time.

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Minor - Minor releases incorporate a number of fixes for known problems into the baseline, or trusted state, of an item. Minor releases usually increment the version number at the first decimal place. For example, version 6.10 would change to version 6.20.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

The following were incorrect answers:

Major - A major release usually introduces new capabilities or functions. Major releases may accumulate all the changes from previous minor releases. Major releases advance the version number by a full increment, for example, from version 5.70 to version 6.

Emergency - Emergency releases are quick fixes to repair unexpected problems or temporary measures to prevent the interruption of critical services.

General software Release – Not a valid type of software release.

Reference:

CISA review manual 2014 Page number 244

Question 1115

Attribute sampling is BEST suited to estimate:

- ☐ compliance with approved procedures.
- ☐ the true monetary value of a population.
- ☐ the total error amount in the population.
- ☒ whether a recorded balance is within limits of materiality.

Licensed to Berend Post berend.post@it-university.nl

Question 1116

Several remote users have been unable to communicate with a secured network news transfer protocol (NNTP) server. Of the following, the MOST likely cause is:

- ☐ the use of a password cracker
- ☒ a hacker impersonating the server
- ☐ a hacker using a sniffer
- ☐ a replay attack by an eavesdropper

Question 1117

An IS auditor should know information about different network transmission media. Which of the following transmission media is used for short distance transmission?

- ☒ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Satellite Radio Link

Explanation:

Explanation:

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Licensed to Berend Post berend.post@it-university.nl

Coaxial Cable

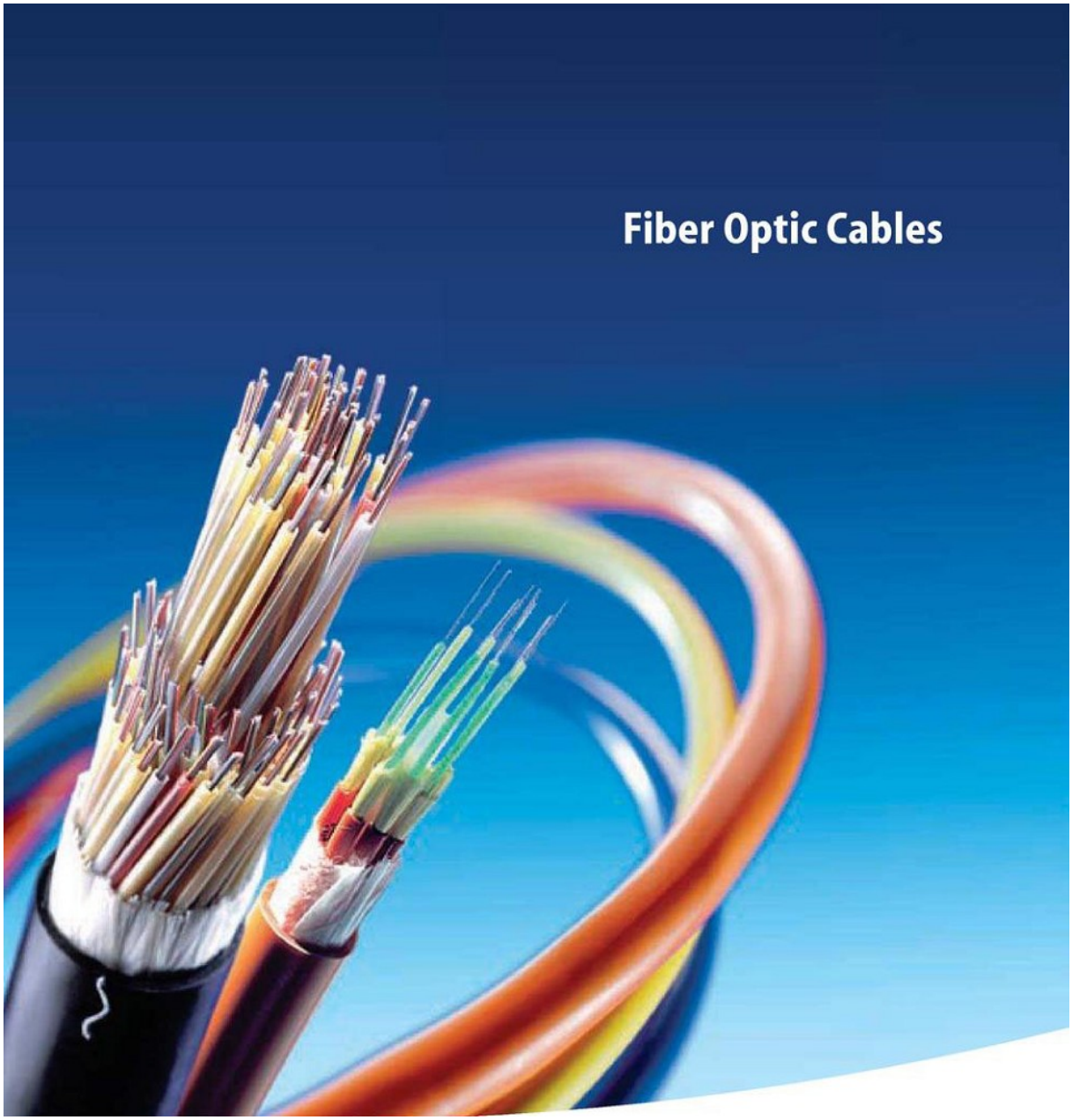
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Microwave radio system

Licensed to Berend Post berend.post@it-university.nl

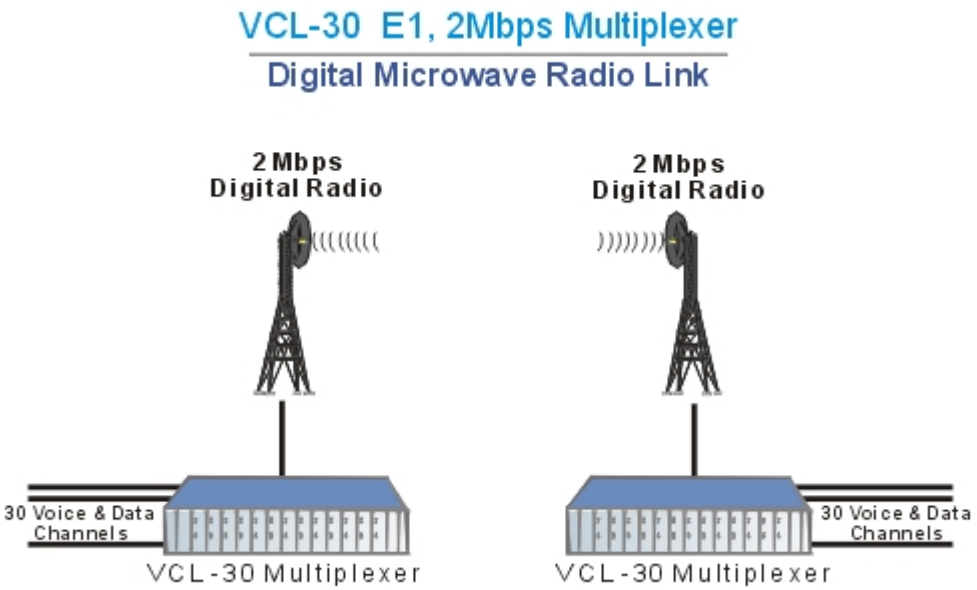
Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

Fiber optics - Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Reference:

CISA review manual 2014 page number 265

Question 1118

Which of the following data validation control validates input data against predefined range values?

- ☒ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Explanation:

Explanation:

In the Range Check control data should not exceed a predefined range of values

For CISA exam you should know below mentioned data validation edits and controls

Sequence Check – The control number follows sequentially and any sequence or duplicated control numbers are rejected or noted on an exception report for follow-up purposes. For example, invoices are numbered sequentially. The day's invoice begins with 12001 and ends with 15045. If any invoice larger than 15045 is encountered during processing, that invoice would be rejected as an invalid invoice number.

Limit Check – Data should not exceed a predefined amount. For example, payroll checks should not exceed US $ 4000. If a check exceeds US $ 4000, data would be rejected for further verification/authorization.

Licensed to Berend Post berend.post@it-university.nl

Validity Check – Programmed checking of data validity in accordance with predefined criteria. For example, a payroll record contains a field for marital status and the acceptable status codes are M or S. If any other code is entered, record should be rejected.

Range Check – Data should not exceed a predefined range of values. For example, product type code range from 100 to 250. Any code outside this range should be rejected as an invalid product type.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Key verification – The keying process is repeated by a separate individual using a machine that compares the original key stroke to the repeated keyed input. For ex. the worker number is keyed twice and compared to verify the keying process.

Check digit – a numeric value that has been calculated mathematically is added to a data to ensure that original data have not been p[altered or incorrect, but Valid, value substituted. This control is effective in detecting transposition and transcription error. For ex. A check digit is added to an account number so it can be checked for accuracy when it is used.

Completeness check – a filed should always contain data rather than zero or blanks. A check of each byte of that field should be performed to determine that some form of data, or not blanks or zeros, is present. For ex. A worker number on a new employee record is left blank. His is identified as a key in filed and the record would be rejected, with a request that the field be completed before the record is accepted for processing.

Duplicate check – new transaction is matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Licensed to Berend Post berend.post@it-university.nl

Logical relationship check – if a particular condition is true, then one or more additional conditions or data input relationship may be required to be true and consider the input valid. For ex. The hire data of an employee may be required to be true and consider the input valid. For ex. The hire date of an employee may be required to be more than 16 years past his her date of birth.

The following were incorrect answers:

Table Lookups – Input data comply with predefined criteria maintained in computerized table of possible values. For example, an input check enters a city code of 1 to 10. This number corresponds with a computerize table that matches a code to a city name.

Existence Check – Data are entered correctly and agree with valid predefined criteria. For example, a valid transaction code must be entered in transaction code field.

Reasonableness check – Input data are matched to predefined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives an order for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program should be designed to print the record with a warning indicating that the order appears unreasonable.

Reference:

CISA review manual 2014 Page number 215

Question 1119

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1120

Which of the following is the BEST way to help ensure new IT implementations align with enterprise architecture principles and requirements?

- ☐ Conduct enterprise architecture reviews as part of the change advisory board.
- ☐ Consider stakeholder concerns when defining the enterprise architecture.
- ☐ Document the security view as part of the enterprise architecture.
- ☒ Perform mandatory post-implementation reviews of IT implementations

Question 1121

In an IS auditor's review of an organization's configuration management practices for software, which of the following is MOST important?

- ☐ Service level agreements (SLAs) between the IT function and users
- ☐ Post-implementation review reports from development efforts
- ☒ Organizational policies related to release management
- ☐ Software rental contracts or lease agreements

Question 1122

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 1123

Which of the following is a directive control?

- ☐ Establishing an information security operations team
- ☐ Updating data loss prevention software
- ☒ Implementing an information security policy
- ☐ Configuring data encryption software

Licensed to Berend Post berend.post@it-university.nl

Question 1124

Which of the following audit techniques is MOST appropriate for verifying application program controls?

- ☐ Statistical sampling
- ☐ Code review
- ☐ Confirmation of accounts
- ☒ Use of test data

Question 1125

An organization is choosing key performance indicators (KPIs) for its information security management. Which of the following KPIs would provide stakeholders with the MOST useful information about whether information security risk is being managed?

- ☐ Time from initial reporting of an incident to appropriate escalation
- ☒ Time from identifying a security threat to implementing a solution
- ☐ The number of security controls implemented
- ☐ The number of security incidents during the past quarter

Question 1126

An IS auditor performing a review of an application's controls would evaluate the:

- ☐ efficiency of the application in meeting the business processes.
- ☒ impact of any exposures discovered.
- ☐ business processes served by the application.
- ☐ application's optimization.

Explanation:

Explanation:

An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

Question 1127

Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

- ☐ A user from within could send a file to an unauthorized person.
- ☐ FTP services could allow a user to download files from unauthorized sources.
- ☒ A hacker may be able to use the FTP service to bypass the firewall.
- ☐ FTP could significantly reduce the performance of a DMZ server.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Since file transfer protocol (FTP) is considered an insecure protocol, it should not be installed on a server in a demilitarized zone (DMZ). FTP could allow an unauthorized user to gain access to the network. Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

Question 1128

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- ☐ A sufficient quantity of data for each test case
- ☒ Data representing conditions that are expected in actual processing
- ☐ Completing the test on schedule
- ☐ A random sample of actual data

Explanation:

Explanation: Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity. It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

Question 1129

Which of the following would be the MOST effective control to reduce the risk of information leakage through social media?

- ☐ Use of keystroke loggers
- ☐ Periodic review of the data classification policy
- ☐ Limited access to social media sites in the workplace
- ☒ Security awareness training

Question 1130

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

Licensed to Berend Post berend.post@it-university.nl

Question 1131

Which of the following exposures could be caused by a line grabbing technique?

- ☒ Unauthorized data access
- ☐ Excessive CPU cycle usage
- ☐ Lockout of terminal polling
- ☐ Multiplexor control dysfunction

Explanation:

Explanation:

Line grabbing will enable eavesdropping, thus allowing unauthorized data access, it will not necessarily cause multiplexor dysfunction, excessive CPU usage or lockout of terminal polling.

Question 1132

When reviewing business continuity plan (BCP) test results, it is MOST important for the IS auditor to determine whether the test:

- ☒ verifies the ability to resume key business operations.
- ☐ considers changes to the systems environment.
- ☐ assesses the capability to retrieve vital records.
- ☐ follows up on activities that occurred since the previous test.

Question 1133

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1134

Which of the following is a technique that could be used to capture network user passwords?

- ☐ Encryption
- ☒ Sniffing
- ☐ Spoofing
- ☐ Data destruction

Explanation:

Explanation: Sniffing is an attack that can be used to capture sensitive pieces of information (e.g., a password) passing through the network. Encryption is a method of scrambling information to prevent unauthorized individuals from understanding the transmission. Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication. Data destruction is erasing information or removing it from its original location.

Question 1135

An organization's audit charter should:

- ☐ set the enterprise strategic direction.
- ☒ detail the audit objectives.
- ☐ define the auditors' right to access information.
- ☐ include the IS audit plan.

Question 1136

Cross-site scripting (XSS) attacks are BEST prevented through:

- ☐ use of common industry frameworks.
- ☒ secure coding practices.
- ☐ application firewall policy settings.
- ☐ a three-tier web architecture.

Question 1137

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

Licensed to Berend Post berend.post@it-university.nl

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 1138

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 1139

Which of the following would be the GREATEST concern to an IS auditor reviewing a critical spreadsheet during a financial audit?

- ☐ Periodic access reviews are manually performed.
- ☒ Changes to the file are not always documented.
- ☐ Access requests are manually processed.
- ☐ A copy current validated file is not available.

Question 1140

Which of the following is the BEST source of information for an IS auditor to use when determining whether an organization's information security policy is adequate?

- ☐ Industry benchmarks
- ☐ Information security program plans
- ☐ Penetration test results
- ☒ Risk assessment results

Licensed to Berend Post berend.post@it-university.nl

Question 1141

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 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 1142

Which of the following BEST supports the risk assessment process to determine criticality of an asset?

- ☐ Threat assessment
- ☐ Residual risk analysis
- ☐ Vulnerability assessment
- ☒ Business impact analysis (BIA)

Licensed to Berend Post berend.post@it-university.nl

Question 1143

While auditing an IT department's cloud service provider, the IS auditor found that privileged access monitoring is not being performed as required by the contract. The provider disagrees with this issue and notes that compensating controls are in place. The IS auditor's NEXT course of action should be to:

- ☒ test compensating controls as part of the audit.
- ☐ define a remediation plan.
- ☐ review privileged access logs.
- ☐ recommend revising the service level agreement (SLA).

Question 1144

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:

Explanation:

The word INCORRECT is the keyword used in the question.

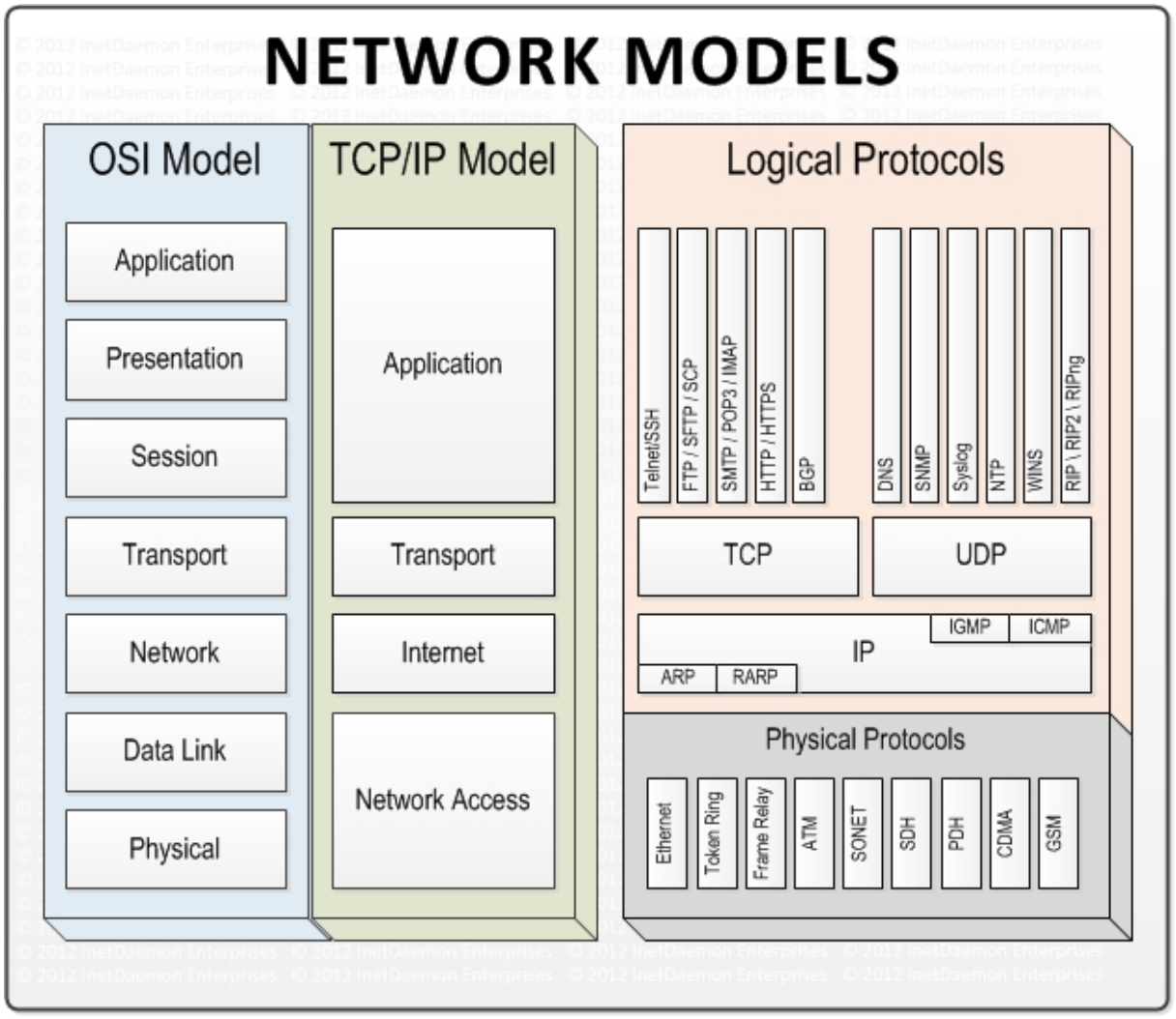
You need to find out invalid layer-protocol mapping.

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.

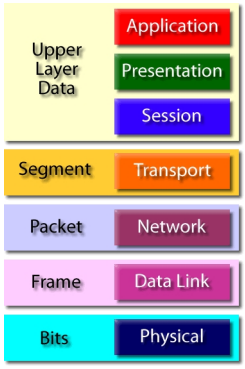
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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):



The following answers are incorrect:

The other options correctly describe layer-protocol mapping in TCP/IP protocol.

Reference:

CISA review manual 2014 page number 272

Question 1145

Which of the following MUST be included in emergency change control procedures?

- ☒ Obtaining user management approval before implementing the changes
- ☐ Updating production source libraries to reflect the changes
- ☐ Using an emergency ID to move production programs into development
- ☐ Requesting that the help desk makes the changes

Question 1146

Which of the following is the GREATEST security risk associated with data migration from a legacy HR system to a cloud-based system?

- ☐ System performance may be impacted by the migration.
- ☐ Records past their retention period may not be migrated to the new system.
- ☐ Data from the source and target system may have different data formats.
- ☒ Data from the source and target system may be intercepted.

Licensed to Berend Post berend.post@it-university.nl

Question 1147

The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- ☒ make unauthorized changes to the database directly, without an audit trail.
- ☐ make use of a system query language (SQL) to access information.
- ☐ remotely access the database.
- ☐ update data without authentication.

Explanation:

Explanation:

Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information, in a networked environment, accessing the database remotely does not make a difference.

What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user ID.

Question 1148

Which of the following would be MOST time and cost efficient when performing a control self-assessment (CSA) for an organization with a large number of widely dispersed employees?

- ☐ Top-down and bottom-up analysis
- ☐ Face-to-face interviews
- ☒ Survey questionnaire
- ☐ Facilitated workshops

Question 1149

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

Licensed to Berend Post berend.post@it-university.nl

Question 1150

When developing a business continuity plan (BCP), business unit management's involvement is MOST important during the:

- ☐ performance of a business impact analysis (BIA).
- ☒ development of business recovery procedures.
- ☐ implementation of a document repository.
- ☐ performance of an IT risk assessment.

Question 1151

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- ☐ O/S and hardware refresh frequencies
- ☒ Gain-sharing performance bonuses
- ☐ Penalties for noncompliance
- ☐ Charges tied to variable cost metrics

Explanation:

Explanation:

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

Question 1152

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

Licensed to Berend Post berend.post@it-university.nl

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

Licensed to Berend Post berend.post@it-university.nl

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Licensed to Berend Post berend.post@it-university.nl

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Deterrent - Deterrent controls are intended to discourage a potential attacker

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

Reference:

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 1153

Which of the following attacks targets the Secure Sockets Layer (SSL)?

- ☒ Man-in-the middle
- ☐ Dictionary
- ☐ Password sniffing
- ☐ Phishing

Explanation:

Explanation:

Attackers can establish a fake Secure Sockets Layer (SSL) server to accept user's SSL traffic and then route to the real SSL server, so that sensitive information can be discovered. A dictionary attack that has been launched to discover passwords would not attack SSL since SSL does not rely on passwords. SSL traffic is encrypted; thus it is not possible to sniff the password. A phishing attack targets a user and not SSL Phishing attacks attempt to have the user surrender private information by falsely claiming to be a trusted person or enterprise.

Question 1154

During an audit of a telecommunications system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:

- ☒ encryption.
- ☐ callback modems.
- ☐ message authentication.
- ☐ dedicated leased lines.

Explanation:

Explanation:

Encryption of data is the most secure method. The other methods are less secure, with leased lines being possibly the least secure method.

Question 1155

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

Licensed to Berend Post berend.post@it-university.nl

Question 1156

Which of the following findings should be an IS auditor's GREATEST concern when reviewing an organization's purchase of new IT infrastructure hardware?

- ☐ The new infrastructure arrived with default system settings.
- ☐ The new infrastructure has residual risk within the organization's risk tolerance.
- ☐ The new infrastructure's hardening requirements are stronger than required by policy.
- ☒ The new infrastructure has compatibility issues with existing systems.

Question 1157

Which of the following is the MOST reasonable option for recovering a noncritical system?

- ☐ Warm site
- ☐ Mobile site
- ☐ Hot site
- ☒ Cold site

Explanation:

Explanation:

Generally, a cold site is contracted for a longer period at a lower cost. Since it requires more time to make a cold site operational, it is generally used for noncritical applications. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any cold or warm site depending upon the need. The need for a mobile site depends upon the scale of operations. A hot site is contracted for a shorter time period at a higher cost and is better suited for recovery of vital and critical applications.

Question 1158

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1159

Which of the following is the BEST approach to reduce unnecessary duplication of compliance activities?

- ☐ Integrating of assurance efforts
- ☐ Automation of controls
- ☒ Standardization of compliance requirements
- ☐ Documentation of control procedures

Question 1160

Which of the following is the MOST important objective of data protection?

- ☐ identifying persons who need access to information
- ☒ Ensuring the integrity of information
- ☐ Denying or authorizing access to the IS system
- ☐ Monitoring logical accesses

Explanation:

Explanation:

Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

Question 1161

An IS auditor has just completed a physical access review of the organization's primary data center. Which of the following weaknesses should be of MOST concern?

- ☐ Metal keys are used for access.
- ☐ Backups of video cameras are corrupt.
- ☒ There is no mantrap at the main door.
- ☐ There is no manual logging for visitors.

Question 1162

Which of the following statement correctly describes difference between SSL and S/HTTP?

- ☐ Both works at application layer of OSI model
- ☒ SSL works at transport layer where as S/HTTP works at application layer of OSI model
- ☐ Both works at transport layer
- ☐ S/HTTP works at transport layer where as SSL works at the application layer of OSI model

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below information about S/HTTP and SSL protocol:

Secure Hypertext Transfer Protocol (S/HTTP) -As an application layer protocol, S/HTTP transmits individual messages or pages securely between a web client and server by establishing SSL-type connection. Using the https:// designation in the URL, instead of the standard http://, directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than the session-oriented protocol.

Secure Socket Layer (SSL) and Transport Layer Security (TLS) - These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases

Peer negotiation for algorithm support

Public-key, encryption based key exchange and certificate based authentication

Symmetric cipher based traffic encryption.

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

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:

Licensed to Berend Post berend.post@it-university.nl

The other choices presented in the options are not valid asSSL works at transport layer where as S/HTTP works at application layer of OSI model.

Reference:

CISA review manual 2014 Page number 352

Question 1163

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 1164

Which of the following processes are performed during the design phase of the systems development life cycle (SDLC) model?

- ☐ Develop test plans.
- ☒ Baseline procedures to prevent scope creep.
- ☐ Define the need that requires resolution, and map to the major requirements of the solution.
- ☐ Program and test the new system. The tests verify and validate what has been developed.

Explanation:

Explanation:

Procedures to prevent scope creep are baselined in the design phase of the systems- development life cycle (SDLC) model.

Licensed to Berend Post berend.post@it-university.nl

Question 1165

What is the BEST population to select from when testing that programs are migrated to production with proper approval?

- ☐ List of changes provided by application programming managers
- ☐ List of production programs
- ☒ Completed change request forms
- ☐ Change advisory board meeting minutes

Question 1166

What is an IS auditor's BEST course of action when provided with a status update indicating audit recommendations related to segregation of duties for financial staff have been implemented?

- ☒ Verify sufficient segregation of duties controls are in place.
- ☐ Request documentation of the segregation of duties policy and procedures.
- ☐ Note the department's response in the audit workpapers and records.
- ☐ Confirm with the business that the recommendations are implemented.

Question 1167

Which of the following is the BEST method to maintain an audit trail of changes made to the source code of a program?

- ☐ Standardize file naming conventions.
- ☒ Utilize automated version control.
- ☐ Document details on a change register.
- ☐ Embed details within source code.

Question 1168

In the context of physical access control, what is known as the process of verifying user identities?

- ☒ Authentication
- ☐ Authorization
- ☐ Accounting
- ☐ Encryption
- ☐ Compression
- ☐ None of the choices.

Explanation:

Explanation:

Authentication is the process of verifying a user's claimed identity. It is based on at least one of these three factors: Something you know, Something you have, or Something you are.

Licensed to Berend Post berend.post@it-university.nl

Question 1169

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 1170

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data- calculation procedures. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

Question 1171

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

- ☒ Cold site
- ☐ Hot site
- ☐ Alternate site
- ☐ Warm site

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A cold site is often an acceptable solution for preparing for recovery of noncritical systems and data.

Question 1172

An organization's disaster recovery plan should address early recovery of:

- ☐ all information systems processes.
- ☐ all financial processing applications.
- ☐ only those applications designated by the IS manager.
- ☒ processing in priority order, as defined by business management.

Explanation:

Explanation:

Business management should know which systems are critical and when they need to process well in advance of a disaster. It is management's responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

Question 1173

An organization has implemented an enhanced password policy for business applications which requires significantly more business unit resources to support clients. The BEST approach to obtain the support of business unit management would be to:

- ☐ elaborate on the positive impact to information security.
- ☐ present industry benchmarking results to business units.
- ☒ discuss the risk and impact of security incidents if not implemented.
- ☐ present an analysis of the cost and benefit of the changes.

Question 1174

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1175

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

- ☐ The use of diskless workstations
- ☒ Periodic checking of hard drives
- ☐ The use of current antivirus software
- ☐ policies that result in instant dismissal if violated

Explanation:

Explanation:

The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded to the network. Antivirus software will not necessarily identify illegal software, unless the software contains a virus. Diskless workstations act as a preventive control and are not effective, since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

Question 1176

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 1177

Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs (choose the most precise answer)?

- ☒ rootkits
- ☐ virus
- ☐ trojan
- ☐ tripwire
- ☐ None of the choices.

Explanation:

Explanation:

"A backdoor may take the form of an installed program (e.g., Back Orifice) or could be in the form of an existing ""legitimate"" program, or executable file. A specific form of backdoors are rootkits, which replaces system binaries and/or hooks into the function calls of the operating system to hide the presence of other programs, users, services and open ports."

Question 1178

Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

- ☐ Minimum operating requirements
- ☒ Acceptable data loss
- ☐ Mean time between failures
- ☐ Acceptable time for recovery

Explanation:

Explanation:

Recovery time objectives (RTOs) are the acceptable time delay in availability of business operations, while recovery point objectives (RPOs) are the level of data loss/reworking an organization is willing to accept. Mean time between failures and minimum operating requirements help in defining recovery strategies.

Question 1179

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:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

An Interrupt attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call.

Example: A boot sector virus typically issues an interrupt to execute a write to the boot sector.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

Traffic analysis - is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. In general, the greater the number of messages observed, or even intercepted and stored, the more can be inferred from the traffic. Traffic analysis can be performed in the context of military intelligence, counter-intelligence, or pattern-of-life analysis, and is a concern in computer security.

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.

Reference:

CISA review manual 2014 Page number 322

Licensed to Berend Post berend.post@it-university.nl

Question 1180

During a review of an application system, an IS auditor identifies automated controls designed to prevent the entry of duplicate transactions. What is the BEST way to verify that the controls work as designed?

- ☒ Implement periodic reconciliations.
- ☐ Review quality assurance (QA) test results.
- ☐ Use generalized audit software for seeking data corresponding to duplicate transactions.
- ☐ Enter duplicate transactions in a copy of the live system.

Question 1181

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- ☐ Test data
- ☒ Generalized audit software
- ☐ Integrated test facility
- ☐ Embedded audit module

Explanation:

Explanation:

Generalized audit software features include mathematical computations, stratification, statistical analysis, sequence checking, duplicate checking and recomputations. An IS auditor, using generalized audit software, could design appropriate tests to recompute the payroll, thereby determining if there were overpayments and to whom they were made. Test data would test for the existence of controls that might prevent overpayments, but it would not detect specific, previous miscalculations. Neither an integrated test facility nor an embedded audit module would detect errors for a previous period.

Question 1182

Which of the following is the BEST practice to ensure that access authorizations are still valid?

- ☐ information owner provides authorization for users to gain access
- ☒ identity management is integrated with human resource processes
- ☐ information owners periodically review the access controls
- ☐ An authorization matrix is used to establish validity of access

Explanation:

Explanation:

Personnel and departmental changes can result in authorization creep and can impact the effectiveness of access controls. Many times when personnel leave an organization, or employees are promoted, transferred or demoted, their system access is not fully removed, which increases the risk of unauthorized access. The best practices for ensuring access authorization is still valid is to

Licensed to Berend Post berend.post@it-university.nl

integrate identity management with human resources processes. When an employee transfers to a different function, access rights are adjusted at the same time.

Question 1183

Which of the following penetration tests would MOST effectively evaluate incident handling and response capabilities of an organization?

- ☐ Targeted testing
- ☐ External testing
- ☐ internal testing
- ☒ Double-blind testing

Explanation:

Explanation:

In a double-blind test, the administrator and security staff are not aware of the test, which will result in an assessment of the incident handling and response capability in an organization. In targeted, external, and internal testing, the system administrator and security staff are aware of the tests since they are informed before the start of the tests.

Question 1184

An IT strategic plan that BEST leverages IT in achieving organizational goals will include:

- ☐ a risk-based ranking of projects.
- ☒ a comparison of future needs against current capabilities.
- ☐ IT budgets linked to the organization's budget.
- ☐ enterprise architecture impacts.

Question 1185

Which of the following ensures the availability of transactions in the event of a disaster?

- ☐ Send tapes hourly containing transactions offsite,
- ☐ Send tapes daily containing transactions offsite.
- ☐ Capture transactions to multiple storage devices.
- ☒ Transmit transactions offsite in real time.

Explanation:

Explanation:

The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

Licensed to Berend Post berend.post@it-university.nl

Question 1186

An IS auditor seeks assurance that a new process for purging transactions does not have a detrimental impact on the integrity of a database. This could be achieved BEST by analyzing the:

- ☐ database structure.
- ☐ design of triggers.
- ☐ results of the process in a test environment.
- ☒ entity relationship diagram of the database.

Question 1187

Which of the following type of a computer network are variation of LAN and are dedicated to connecting storage devices to servers and other computing devices?

- ☐ LAN
- ☐ MAN
- ☒ SAN
- ☐ PAN

Explanation:

Explanation:

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

For your exam you should know below information about computer networks:

Local Area Network (LAN)

A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

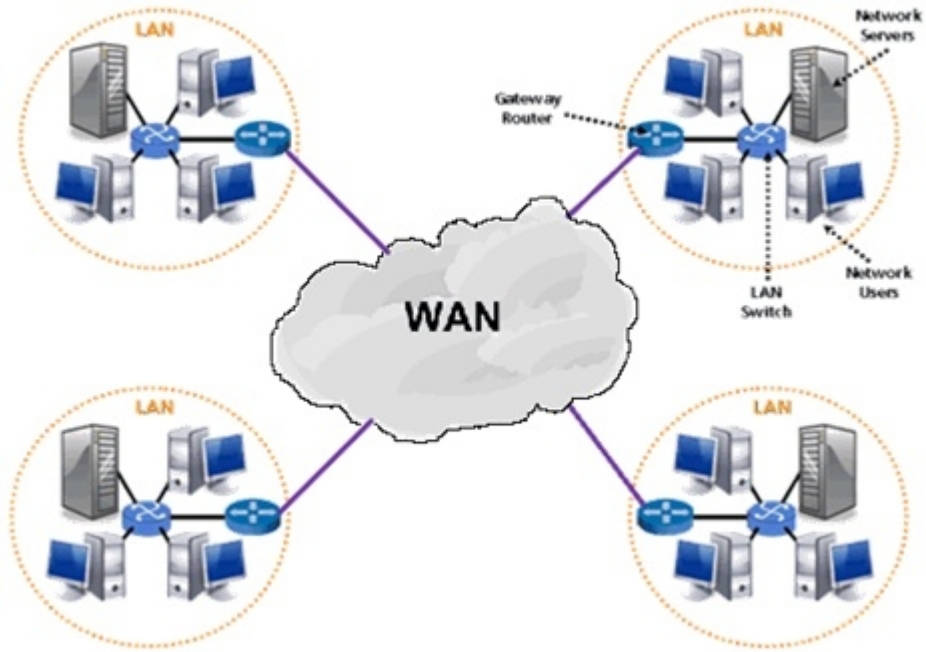
Local Area Network

Licensed to Berend Post berend.post@it-university.nl

Wide Area Network

A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.

Wide Area Network

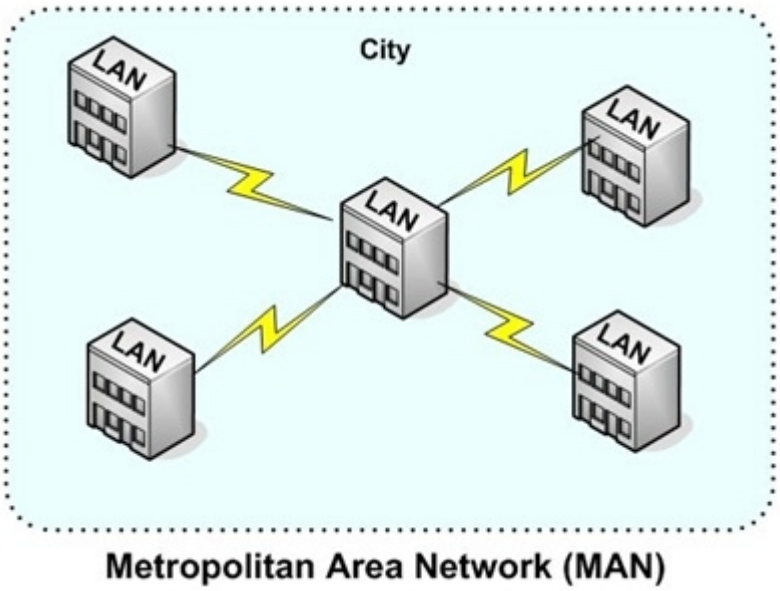


Metropolitan Area Network

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Metropolitan Area Network

Licensed to Berend Post berend.post@it-university.nl

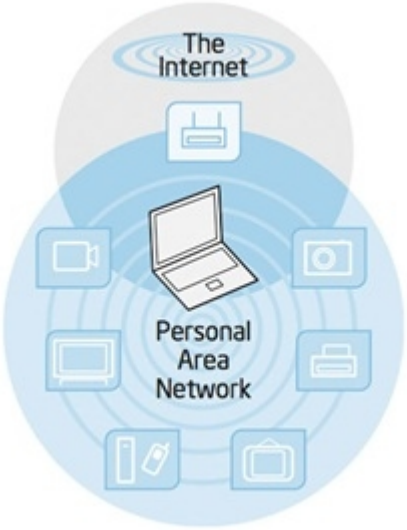


Metropolitan Area Network (MAN)

Personal Area Network

A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

Personal Area Network



Storage Area Network

A storage area network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices, such as disk arrays, tape libraries, and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to

Licensed to Berend Post berend.post@it-university.nl

the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

Storage Area Network

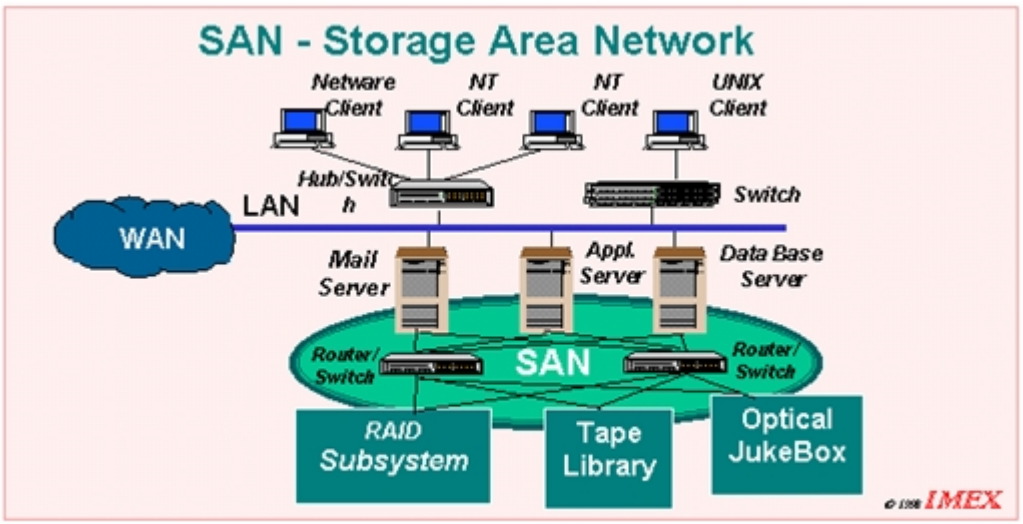


Figure – 3: SAN – Dedicated Storage Area Network dedicated to data movement between servers and storage or between diverse storage devices or between any nodes attached to the SAN.

The following were incorrect answers:

PAN - A personal area network (PAN) is a computer network used for data transmission among devices such as computers, telephones and personal digital assistants. PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink).

LAN - A local area network (LAN) is a computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building using network media.

MAN - A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. Metropolitan limits are determined by local municipal corporations; the larger the city, the bigger the MAN, the smaller a metro city, smaller the MAN

Reference:

CISA review manual 2014 Page number 258

Licensed to Berend Post berend.post@it-university.nl

Question 1188

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 1189

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1190

For an organization which uses a VoIP telephony system exclusively, the GREATEST concern associated with leaving a connected telephone in an unmonitored public area is the possibility of:

- ☐ connectivity issues when used with an analog local exchange carrier
- ☒ unauthorized use leading to theft of services and financial loss
- ☐ network compromise due to the introduction of malware
- ☐ theft or destruction of an expensive piece of electronic equipment

Question 1191

The ability of the internal IS audit function to achieve desired objectives depends largely on:

- ☐ the training of audit personnel
- ☐ the background of audit personnel
- ☒ the independence of audit personnel
- ☐ the performance of audit personnel
- ☐ None of the choices.

Explanation:

Explanation:

The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Top management should ensure that the audit department does not participate in activities that may compromise its independence.

Question 1192

Which of the following tests would provide the BEST assurance that a health care organization is handling patient data appropriately?

- ☐ Compliance with local laws and regulations
- ☐ Compliance with the organization's policies and procedures
- ☒ Compliance with action plans resulting from recent audits
- ☐ Compliance with industry standards and best practice

Licensed to Berend Post berend.post@it-university.nl

Question 1193

You are part of a security staff at a highly profitable bank and each day, all traffic on the network is logged for later review. Every Friday when major deposits are made you're seeing a series of bits placed in the "Urgent Pointer" field of a TCP packet. This is only 16 bits which isn't much but it concerns you because:

☒ This could be a sign of covert channeling in bank network communications and should be investigated.
☐ It could be a sign of a damaged network cable causing the issue.
☐ It could be a symptom of malfunctioning network card or drivers and the source system should be checked for the problem.
☐ It is normal traffic because sometimes the previous fields 16-bit checksum value can over run into the urgent pointer's 16-bit field causing the condition.

Explanation:

Explanation:

The Urgent Pointer is used when some information has to reach the server ASAP. When the TCP/IP stack at the other end sees a packet using the Urgent Pointer set, it is duty bound to stop all ongoing activities and immediately send this packet up the stack for immediate processing. Since the packet is plucked out of the processing queue and acted upon immediately, it is known as an Out Of Band (OOB)packet and the data is called Out Of Band (OOB) data.

The Urgent Pointer is usually used in Telnet, where an immediate response (e.g. the echoing of characters) is desirable.

Covert Channels are not directly synonymous with backdoors. A covert channel is simply using a communication protocol in a way it was not intended to be used or sending data without going through the proper access control mechanisms or channels. For example, in a Mandatory Access Control systems a user at secret has found a way to communicate information to a user at Confidential without going through the normal channels.

In this case the Urgent bit could be used for a few reasons:

1. It could be to attempt a Denial of service where the host receiving a packet with the Urgent bit set will give immediate attention to the request and will be in wait state until the urgent message is receive, if the sender does not send the urgent message then it will simply sit there doing nothing until it times out. Some of the TCP/IP stacks used to have a 600 seconds time out, which means that for 10 minutes nobody could use the port. By sending thousands of packet with the URGENT flag set, it would create a very effective denial of service attack.

Licensed to Berend Post berend.post@it-university.nl

2. It could be used as a client server application to transmit data back and forward without going through the proper channels. It would be slow but it is possible to use reserved fields and bits to transmit data outside the normal communication channels.

The other answers are incorrect

Reference:

http://www.fas.org/irp/nsa/rainbow/tg030.htm document covering the subject of covert channels

and also see:

http://gray-world.net/papers.shtml which is a large collection of documents on Covert Channels

Question 1194

What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

- ☐ A combination of public-key cryptography and digital certificates and two-factor authentication
- ☐ A combination of public-key cryptography and two-factor authentication
- ☒ A combination of public-key cryptography and digital certificates
- ☐ A combination of digital certificates and two-factor authentication

Explanation:

Explanation:

PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

Question 1195

Which of the following should be done FIRSTwhen handling multiple confirmed incidents raised at the same time?

- ☒ Categorize incidents by the value of the affected asset.
- ☐ Inform senior management.
- ☐ Update the business impact assessment.
- ☐ Activate the business continuity plan.

Licensed to Berend Post berend.post@it-university.nl

Question 1196

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 1197

Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

- ☐ Backup time would steadily increase
- ☐ Backup operational cost would significantly increase
- ☐ Storage operational cost would significantly increase
- ☒ Server recovery work may not meet the recovery time objective (RTO)

Explanation:

Explanation:

In case of a crash, recovering a server with an extensive amount of data could require a significant amount of time. If the recovery cannot meet the recovery time objective (RTO), there will be a discrepancy in IT strategies. It's important to ensure that server restoration can meet the RTO. Incremental backup would only take the backup of the daily differential, thus a steady increase in backup time is not always true. The backup and storage costs issues are not as significant as not meeting the RTO.

Question 1198

To preserve chain of custody following an internal server compromise, which of the following should be the FIRST step?

- ☒ Take a system image including memory dump
- ☐ Safely shut down the server
- ☐ Replicate the attack using the remaining evidence
- ☐ Trace the attacking route

Licensed to Berend Post berend.post@it-university.nl

Question 1199

Which of the following conditions would be of MOST concern to an IS auditor assessing the risk of a successful brute force attack encrypted data at rest?

- ☐ Use of symmetric encryption
- ☐ Use of asymmetric encryption
- ☐ Random key generation
- ☒ Short key length

Question 1200

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:

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.

Licensed to Berend Post berend.post@it-university.nl

Telnet or Remote Terminal Control Protocol -A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session, you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Internet Link- Internet link is a connection between Internet users and the Internet service provider.

Secure Shell or Secure Socket Shell (SSH) - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Domain Name System (DNS) - The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name System.

File Transfer Protocol (FTP) - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates 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.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

SMTP - Simple Mail Transport Protocol (SMTP) - SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail. On Unix-based systems, send mail is the most widely-used SMTP server for e-mail. A commercial package, Send mail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

FTP - The File Transfer Protocol or FTP is a client/server application that is used to move files from one system to another. The client connects to the FTP server, authenticates and is given access that the server is configured to permit. FTP servers can also be configured to allow anonymous access by logging in with an email address but no password. Once connected, the client may move around between directories with commands available

SSH - Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slog in, sash, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rash, and rap. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

Reference:

CISA review manual 2014 page number 273 and 274

Question 1201

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

Licensed to Berend Post berend.post@it-university.nl

Question 1202

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.

Reference:

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 1203

Which of the following is MOST important for an IS auditor to verify during a disaster recovery audit?

- ☒ Disaster recovery tests are carries out.
- ☐ Regular backups are made and stored offsite.
- ☐ The disaster recovery plan is updated on a regular basis.
- ☐ Media are stored in fireproof cabinets.

Question 1204

The waterfall life cycle model of software development is most appropriately used when:

- ☒ requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
- ☐ requirements are well understood and the project is subject to time pressures.
- ☐ the project intends to apply an object-oriented design and programming approach.
- ☐ the project will involve the use of new technology.

Explanation:

Explanation:

Historically, the waterfall model has been best suited to the stable conditions described in choice

A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall

Licensed to Berend Post berend.post@it-university.nl

system to be delivered, making the requirements gathering and design activities more manageable. The ability to deliver working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits. The choice of a design and programming approach is not itself a determining factor of the type of software development life cycle that is appropriate. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

Question 1205

Which of the following is the MOST significant concern when backup tapes are encrypted?

- ☒ Loss of the encryption key
- ☐ Lack of physical security over the tapes
- ☐ Incompatibility with future software versions
- ☐ Inaccurate data due to encryption processing

Question 1206

Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

- ☐ Print service, application services
- ☐ Data encryption and compression
- ☐ Dialog management
- ☒ End-to-end connection

Explanation:

Explanation:

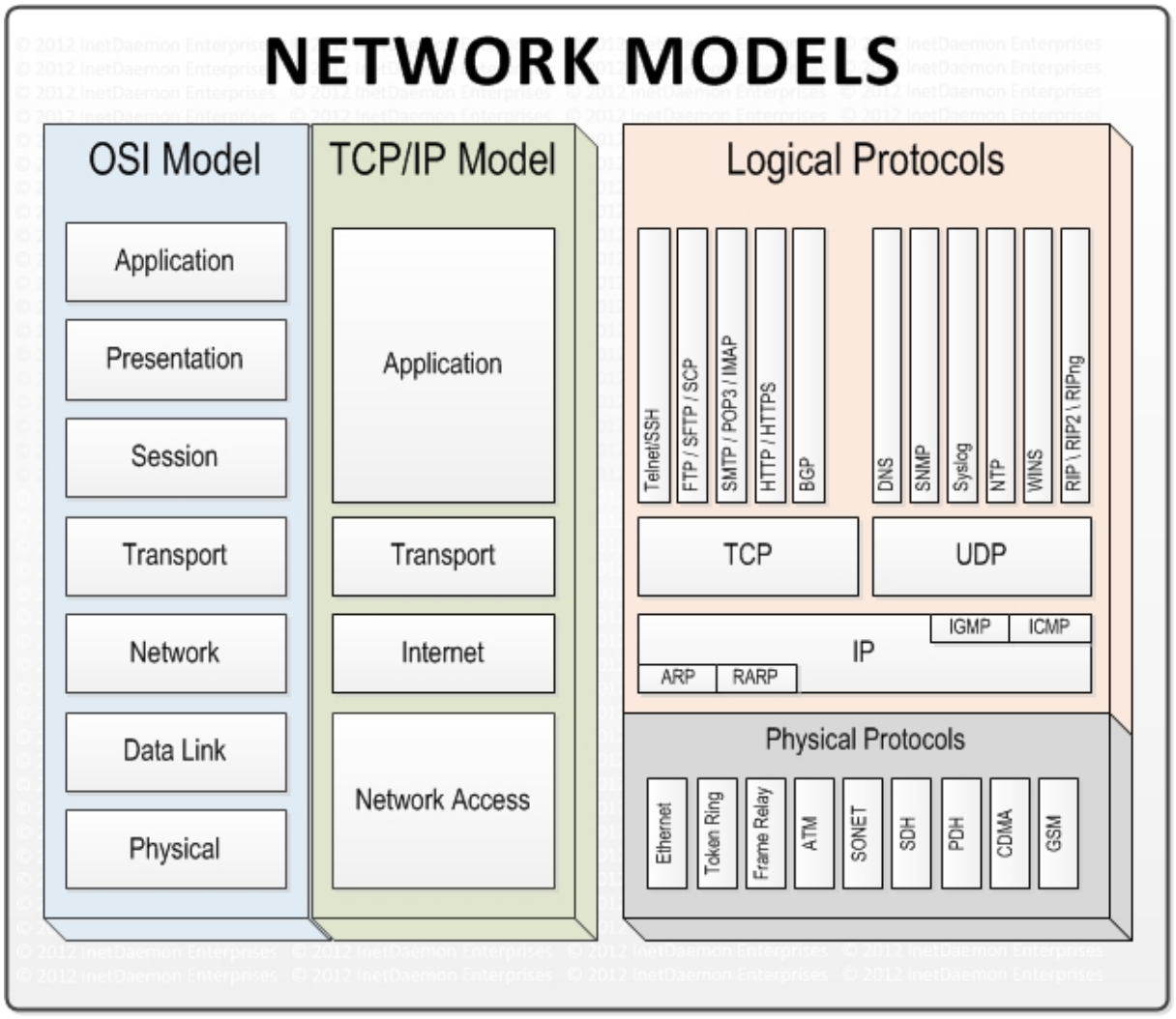
The word NOT is the keyword used in the question. You need to find out a functionality which is not performed by application layer of a TCP/IP model.

End-to-end connection is the Transport layer functionality in TCP/IP model.

For your exam you should know below information about TCP/IP model:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

Licensed to Berend Post berend.post@it-university.nl

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

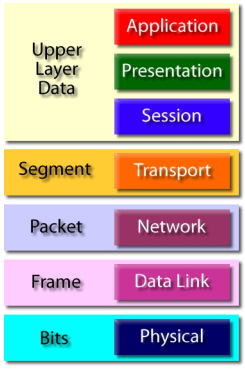
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other,

 Licensed to Berend Post berend.post@it-university.nl

destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

The other functionalities described in the options are performed by application layer in TCP/IP model.

Reference:

CISA review manual 2014 page number 272

Question 1207

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

Licensed to Berend Post berend.post@it-university.nl

Question 1208

Implementing which of the following would BEST address issues relating to the aging of IT systems?

- ☐ IT project management
- ☒ Release management
- ☐ Application portfolio management
- ☐ Configuration management

Question 1209

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 1210

Which of the following is the key benefit of control self-assessment (CSA)?

- ☒ Management ownership of the internal controls supporting business objectives is reinforced.
- ☐ Audit expenses are reduced when the assessment results are an input to external audit work.
- ☐ Improved fraud detection since internal business staff are engaged in testing controls
- ☐ Internal auditors can shift to a consultative approach by using the results of the assessment.

Explanation:

Explanation:

The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance.

Reducing audit expenses is not a key benefit of control self-assessment (CSA). improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

Licensed to Berend Post berend.post@it-university.nl

Question 1211

An organization is moving its on-site application servers to a service provider that operates a virtualized environment shared by multiple customers. Which of the following is the MOST significant risk to the organization?

- ☐ Account hacking from other clients
- ☒ Competing workloads from other clients
- ☐ Service provider access to organizational data
- ☐ Service provider limiting the right to audit

Question 1212

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain an effective information security program?

- ☒ Determine new factors that could influence the information security strategy.
- ☐ Implement the current information security program in the acquired company.
- ☐ Merge the two information security programs to establish continuity.
- ☐ Ensure information security is included in any change control efforts.

Question 1213

Which of the following is the BEST type of backup to minimize the associated time and media?

- ☒ Differential
- ☐ Incremental
- ☐ Mirror
- ☐ Compressed full

Question 1214

An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

- ☐ Analyze the need for the structural change.
- ☐ Recommend restoration to the originally designed structure.
- ☐ Recommend the implementation of a change control process.
- ☒ Determine if the modifications were properly approved.

Explanation:

Explanation:

An IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the IS auditor find that the structural modification had not been approved.

Licensed to Berend Post berend.post@it-university.nl

Question 1215

An organization considers implementing a system that uses a technology that is not in line with the organization's IT strategy. Which of the following is the BEST justification for deviating from the IT strategy?

- ☒ The system has a reduced cost of ownership.
- ☐ The organization has staff familiar with the technology.
- ☐ The business benefits are achieved even with extra costs.
- ☐ The system makes use of state-of-the-art technology.

Question 1216

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 1217

Calculation of the recovery time objective (RTO) is necessary to determine the:

- ☐ time required to restore files.
- ☐ annual loss expectancy (ALE).
- ☐ point of synchronization.
- ☒ priority of restoration.

Licensed to Berend Post berend.post@it-university.nl

Question 1218

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:

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:

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.

Reference:

CISA review manual 2014 Page number 188

Question 1219

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:

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.

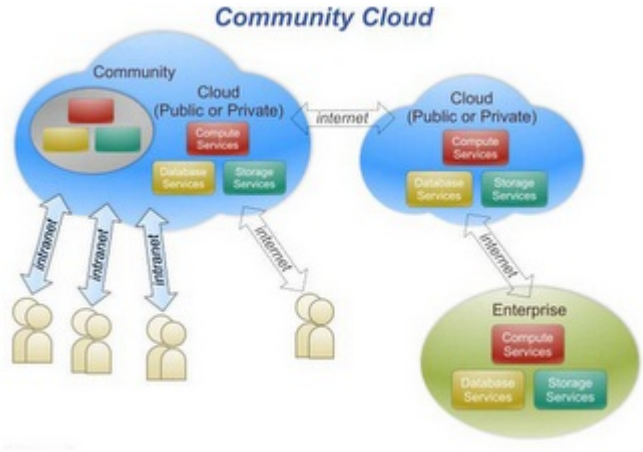
Private Cloud

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

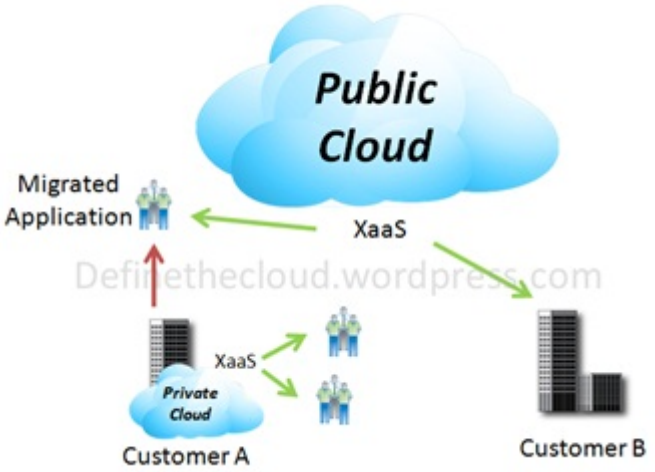


Public Cloud

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

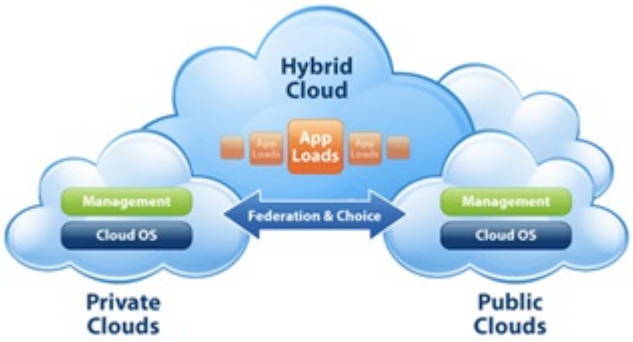
Licensed to Berend Post berend.post@it-university.nl



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)

Reference:

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

Question 1220

There are several types of penetration tests depending upon the scope, objective and nature of a test. Which of the following describes a penetration test where you attack and attempt to circumvent the controls of the targeted network from the outside, usually the Internet?

- ☒ External Testing
- ☐ Internal Testing
- ☐ Blind Testing
- ☐ Targeted Testing

Explanation:

Explanation:

External testing refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system, usually the Internet.

For the CISA exam you should know penetration test types listed below:

External Testing -Refers to attack and control circumvention attempts on a target's network perimeter from outside the target's system, 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 testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Double Blind Testing -It is an extension of blind testing, since the administrator and security staff at the target are also not aware of test. Such a testing can effectively evaluate the incident handling and response capability of the target and how well managed the environment is.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

The following were incorrect answers:

Internal Testing – Refers to attack and control circumvention attempt on target from within the perimeter. The objective is to identify what would occur if the external perimeter was successfully compromised and/or an authorized user from within the network wanted to compromise security of a specific resource on a network.

Blind Testing -Refers to the condition of testing when the penetration tester is provided with limited or no knowledge of the target's information systems. Such a testing is expensive, since penetration tester have to research the target and profile it based on publicly available information.

Targeted Testing – Refers to attack and control circumvention attempts on the target, while both the target's IT team and penetration tester are aware of the testing activities. Penetration testers are provided with information related to target and network design. Additionally, they are also provided with a limited privilege user account to be used as a starting point to identify privilege escalation possibilities in the system.

Reference:

CISA review manual 2014 Page number 369

Licensed to Berend Post berend.post@it-university.nl

Question 1221

A core tenant of an IS strategy is that it must:

- ☐ Be inexpensive
- ☐ Be protected as sensitive confidential information
- ☐ Protect information confidentiality, integrity, and availability
- ☒ Support the business objectives of the organization

Explanation:

Explanation:

Above all else, an IS strategy must support the business objectives of the organization.

Question 1222

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 1223

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- ☐ Optimized
- ☒ Managed
- ☐ Defined
- ☐ Repeatable

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

Question 1224

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 1225

Which of the following should be an information security manager's PRIMARY role when an organization initiates a data classification process?

- ☐ Assign the asset classification level.
- ☒ Define the classification structure to be implemented.
- ☐ Verify that assets have been appropriately classified.
- ☐ Apply security in accordance with specific classification.

Question 1226

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- ☐ the IT infrastructure.
- ☐ organizational policies, standards and procedures.
- ☒ legal and regulatory requirements.
- ☐ the adherence to organizational policies, standards and procedures.

Explanation:

Explanation:

To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to

Licensed to Berend Post berend.post@it-university.nl

determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

Question 1227

Which of the following controls MOST efficiently ensures that orders transmitted from a sales office to a production warehouse are received accurately and completely?

- ☐ Transaction totals and record counts should be sent and reconciled before transaction processing.
- ☒ Parity checking should be incorporated into all data transmissions.
- ☐ Data should be sent back to the originating site and compared to what was sent to production.
- ☐ Continuity of numerical sequences for all sales orders should be checked.

Question 1228

Reports to the executive level concerning IT performance should focus on:

- ☐ third-party compliance with organizational practices.
- ☐ IT performance in relation to operational improvements.
- ☒ IT deliverables against organizational strategies.
- ☐ capacity planning effectiveness within the organization.

Question 1229

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 1230

Which of the following tests is MOST likely to detect an error in one subroutine resulting from a recent change in another subroutine?

- ☐ Stress testing
- ☒ Regression testing
- ☐ User acceptance testing
- ☐ Black-box testing

Question 1231

An organization globally distributes a free phone application that includes a module to gather and report user information. The application includes a privacy notice alerting users to the data gathering. Which of the following presents the GREATEST risk?

- ☐ The data gathering notice is available in only one language.
- ☐ There is no framework to delete personal data.
- ☐ There may be a backlash among users when the data gathering is revealed.
- ☒ The data is not properly encrypted on the application server.

Question 1232

Which of the following should be of GREATEST concern to an IS auditor when auditing an organization's information security awareness program?

- ☒ Security awareness training is not included as part of the onboarding process for new hires.
- ☐ The number of security incidents logged by employees to the help desk has increased in the past year.
- ☐ Training quizzes are designed and run by a third-party company under a contract with the organization.
- ☐ Security awareness training is run via the organization's enterprise-wide e-learning portal.

Question 1233

Which of the following is MOST effective against system intrusions?

- ☐ Continuous monitoring
- ☒ Layered protection
- ☐ Penetration testing
- ☐ Two-factor authentication

Licensed to Berend Post berend.post@it-university.nl

Question 1234

What should an IS auditor review FIRST when assessing the results of a recent penetration test to identify potential vulnerabilities?

- ☐ Skill level of the network support staff
- ☒ Parameters of the test
- ☐ Number of critical issues found
- ☐ Incident response process

Question 1235

A local area network (LAN) administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager
- ☒ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Explanation:

Explanation:

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

Question 1236

Which of the following would be the FIRST step to help ensure the necessary regulatory requirements are addressed in an organization's cross-border data protection policy?

- ☐ Conduct a risk assessment
- ☒ Perform a gap analysis
- ☐ Conduct stakeholder interviews
- ☐ Perform a business impact analysis

Question 1237

Run-to-run totals can verify data through which stage(s) of application processing?

- ☐ Initial
- ☒ Various
- ☐ Final
- ☐ Output

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Run-to-run totals can verify data through various stages of application processing.

Question 1238

A top-down approach to the development of operational policies will help ensure:

- ☒ that they are consistent across the organization.
- ☐ that they are implemented as a part of risk assessment.
- ☐ compliance with all policies.
- ☐ that they are reviewed periodically.

Explanation:

Explanation:

Deriving lower level policies from corporate policies {a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

Question 1239

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

- ☐ Legal
- ☐ Help desk
- ☐ Human resources
- ☒ Information security

Question 1240

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

Reference:

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 1241

Which of the following is the BEST indicator of the effectiveness of signature-based intrusion detection systems?

- ☐ An increase in the number of identified false positives
- ☐ An increase in the number of unfamiliar sources of intruders
- ☒ An increase in the number of detected incidents not previously identified
- ☐ An increase in the number of internally reported critical incidents

Question 1242

In a typical network architecture used for e-commerce, a load balancer is normally found between the:

- ☒ routers and the web servers.
- ☐ mail servers and the mail repositories.
- ☐ users and the external gateways.
- ☐ databases and the external gateways.

Question 1243

Which of the following is the BEST way to address ongoing concerns with the quality and accuracy of internal audits?

- ☒ Engage an independent review of the audit function.
- ☐ Require peer reviews of audit workpapers.
- ☐ Implement performance management for IS auditors.
- ☐ Require IS audit management to lead exit meetings.

Question 1244

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1245

Which of the following would be an IS auditor's GREATEST concern when reviewing the early stages of a software development project?

- ☐ The lack of acceptance criteria behind user requirements
- ☐ The lack of completion of all requirements at the end of each sprint
- ☐ The lack of technical documentation to support the program code
- ☒ The lack of a detailed unit and system test plan

Question 1246

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 1247

An IS auditor has been asked to audit a complex system with computerized and manual elements. Which of the following should be identified FIRST?

- ☐ Manual controls
- ☐ System risks
- ☐ Programmed controls
- ☒ Input validation

Question 1248

An IS auditor evaluating a three-tier client/server architecture observes an issue with graphical user interface (GUI) tasks. Which layer should the auditor recommend the client address?

- ☒ Presentation layer
- ☐ Application layer
- ☐ Storage layer
- ☐ Transport layer

Licensed to Berend Post berend.post@it-university.nl

Question 1249

Which of the following is the GREATEST risk associated with in-house program development and customization?

- ☐ The lack of a test environment
- ☒ The lack of a quality assurance function
- ☐ The lack of secure coding expertise
- ☐ The lack of documentation for programs developed.

Question 1250

Which of the following is the MOST important activity to undertake to avoid rework later in a project?

- ☐ Control review
- ☐ Risk assessment
- ☐ Acceptance testing
- ☒ Phase review

Question 1251

When reviewing an end-user computing (EUC) application, which of the following techniques is MOST appropriate for testing program logic?

- ☐ Integrated testing facility
- ☒ Test decking
- ☐ Re-performance
- ☐ Key calculation inspection

Question 1252

An IS auditor is following upon a finding that determined elevated administrator accounts for servers were not being properly checked out and then back in after each use. Which of the following is the MOST appropriate sampling technique to determine the scope of the problem?

- ☐ Stratified sampling
- ☐ Random sampling
- ☒ Attribute sampling
- ☐ Statistical sampling

Licensed to Berend Post berend.post@it-university.nl

Question 1253

An organization with many desktop PCs is considering moving to a thin client architecture. Which of the following is the MAJOR advantage?

- ☐ Administrative security can be provided for the client.
- ☐ System administration can be better managed.
- ☐ The security of the desktop PC is enhanced.
- ☒ Desktop application software will never have to be upgraded.

Question 1254

Which of the following should be of MOST concern to an IS auditor during the review of a quality management system?

- ☐ The quality management system includes training records for IT personnel.
- ☒ There are no records to document actions for minor business processes.
- ☐ Important quality checklists are maintained outside the quality management system.
- ☐ Indicators are not fully represented in the quality management system.

Question 1255

Which of the following network configuration options contains a direct link between any two host machines?

- ☐ Bus
- ☐ Ring
- ☐ Star
- ☒ Completely connected (mesh)

Explanation:

Explanation:

A completely connected mesh configuration creates a direct link between any two host machines.

Question 1256

IT best practices for the availability and continuity of IT services should:

- ☐ minimize costs associated with disaster-resilient components.
- ☐ provide for sufficient capacity to meet the agreed upon demands of the business.
- ☒ provide reasonable assurance that agreed upon obligations to customers can be met.
- ☐ produce timely performance metric reports.

Explanation:

Explanation:

It is important that negotiated and agreed commitments (i.e., service level agreements [SLAs]) can be fulfilled all the time. If this were not achievable, IT should not have agreed to these requirements, as

Licensed to Berend Post berend.post@it-university.nl

entering into such a commitment would be misleading to the business. 'All the time' in this context directly relates to the 'agreed obligations' and does not imply that a service has to be available 100 percent of the time. Costs are a result of availability and service continuity management and may only be partially controllable. These costs directly reflect the agreed upon obligations. Capacity management is a necessary, but not sufficient, condition of availability.

Despite the possibility that a lack of capacity may result in an availability issue, providing the capacity necessary for seamless operations of services would be done within capacity management, and not within availability management. Generating reports might be a task of availability and service continuity management, but that is true for many other areas of interest as well (e.g., incident, problem, capacity and change management).

Question 1257

Email required for business purposes is being stored on employees' personal devices. Which of the following is an IS auditor's BEST recommendation?

- ☐ Implement an email containerization solution on personal devices
- ☐ Prohibit employees from storing company email on personal devices.
- ☐ Ensure antivirus to utilize passwords on personal devices.
- ☒ Require employees to utilize passwords on personal devices.

Question 1258

Which of the following is the GREATEST risk posed by denial-of-service attacks?

- ☐ Confidential information leakage
- ☐ Loss of integrity and corruption of databases
- ☒ Loss of reputation and business
- ☐ Unauthorized access to the systems

Question 1259

Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

- ☐ Certificate revocation list (CRL)
- ☒ Certification practice statement (CPS)
- ☐ Certificate policy (CP)
- ☐ PKI disclosure statement (PDS)

Explanation:

Explanation:

The CPS is the how-to part in policy-based PKI. The CRL is a list of certificates that have been revoked before their scheduled expiration date. The CP sets the requirements that are subsequently implemented by the CPS. The PDS covers critical items such as the warranties, limitations and obligations that legally bind each party.

Licensed to Berend Post berend.post@it-university.nl

Question 1260

Following a successful attack on an organization's web server, which of the following actions should be performed FIRST?

- ☒ Review the boundary configuration rules to ensure that outbound packets are limited
- ☐ Evaluate and deploy an intrusion detection system
- ☐ Periodically scan the network for systems with well-known vulnerabilities
- ☐ Establish reference systems using cryptographic checksum tools

Question 1261

During the audit of a database server, which of the following would be considered the GREATEST exposure?

- ☐ The password does not expire on the administrator account
- ☒ Default global security settings for the database remain unchanged
- ☐ Old data have not been purged
- ☐ Database activity is not fully logged

Explanation:

Explanation:

Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

Question 1262

Which of the following comparisons are used for identification and authentication in a biometric system?

- ☐ One-to-many for identification and authentication
- ☐ One-to-one for identification and authentication
- ☒ One-to-many for identification and one-to-one for authentication
- ☐ One-to-one for identification and one-to-many for authentication

Explanation:

Explanation:

In identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative

Licensed to Berend Post berend.post@it-university.nl

recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be"

In verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

Management of Biometrics

Management of biometrics should address effective security for the collection, distribution and processing of biometrics data encompassing:

Data integrity, authenticity and non-repudiation

Management of biometric data across its life cycle – compromised of the enrollment, transmission and storage, verification, identification, and termination process

Usage of biometric technology, including one-to-one and one-to-many matching, for identification and authentication

Application of biometric technology for internal and external, as well as logical and physical access control

Encapsulation of biometric data

Security of the physical hardware used throughout the biometric data life cycle

Techniques for integrity and privacy protection of biometric data.

The following were incorrect answers:

All other choices presented were incorrectly describing identification and authentication mapping.

Reference:

CISA review manual 2014 Page number 331

http://en.wikipedia.org/wiki/Biometrics

Licensed to Berend Post berend.post@it-university.nl

Question 1263

Which of the following is the PRIMARY benefit to an organization using an automated event monitoring solution?

- ☐ Enhanced forensic analysis
- ☒ Improved response time to incidents
- ☐ Improved network protection
- ☐ Reduced need for manual analysis

Question 1264

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 1265

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 1266

A retirement system verifies that the field for employee status has either a value of A (for active) or R (for retired). This is an example of which type of check?

- ☒ Validity
- ☐ Existence
- ☐ Limit
- ☐ Completeness

Question 1267

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 1268

A retailer normally uses a scanner to read product labels and input product codes and prices. The unit is not functioning and staff are keying information manually. With respect to the accuracy of the input, it is likely that:

- ☐ audit risk has increased.
- ☐ control risk has increased.
- ☒ inherent risk has decreased.
- ☐ detection risk has decreased.

Question 1269

Which of the following is the safest means of transmitting confidential information over the Internet?

- ☐ Send the data to a trusted third party to resend to the destination.
- ☐ Use asymmetric encryption and encrypt the data with a private key.
- ☒ Establish a virtual private network (VPN) between the source and the destination.
- ☐ Break the data into many packets and send it over different routes.

Licensed to Berend Post berend.post@it-university.nl

Question 1270

Which of the following is MOST important with regard to an application development acceptance test?

- ☐ The quality assurance (QA) team is in charge of the testing process.
- ☐ User management approves the test design before the test is started.
- ☐ The programming team is involved in the testing process.
- ☒ All data files are tested for valid information before conversion.

Question 1271

Which of the following scenarios would enable a forensic investigation?

- ☒ The suspected computer was rebooted, and the evidence log file was converted to a readable format for further analysis.
- ☐ The incident response team prepared a final report for the forensic investigator and deleted the original file securely to avoid further damage.
- ☐ The media in question was preserved using imaging, and chain of custody was documented according to the organization's incident response plan.
- ☐ Incident response team members extracted the logs showing the suspicious activity and added their notes before submitting for investigation.

Question 1272

Which of the following transmission media uses a transponder to send information?

- ☐ Copper cable
- ☐ Fiber Optics
- ☒ Satellite Radio Link
- ☐ Coaxial cable

Explanation:

Explanation:

Satellite radio link uses transponder to send information and are easy to intercept.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Licensed to Berend Post berend.post@it-university.nl

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Licensed to Berend Post berend.post@it-university.nl

Coaxial Cable

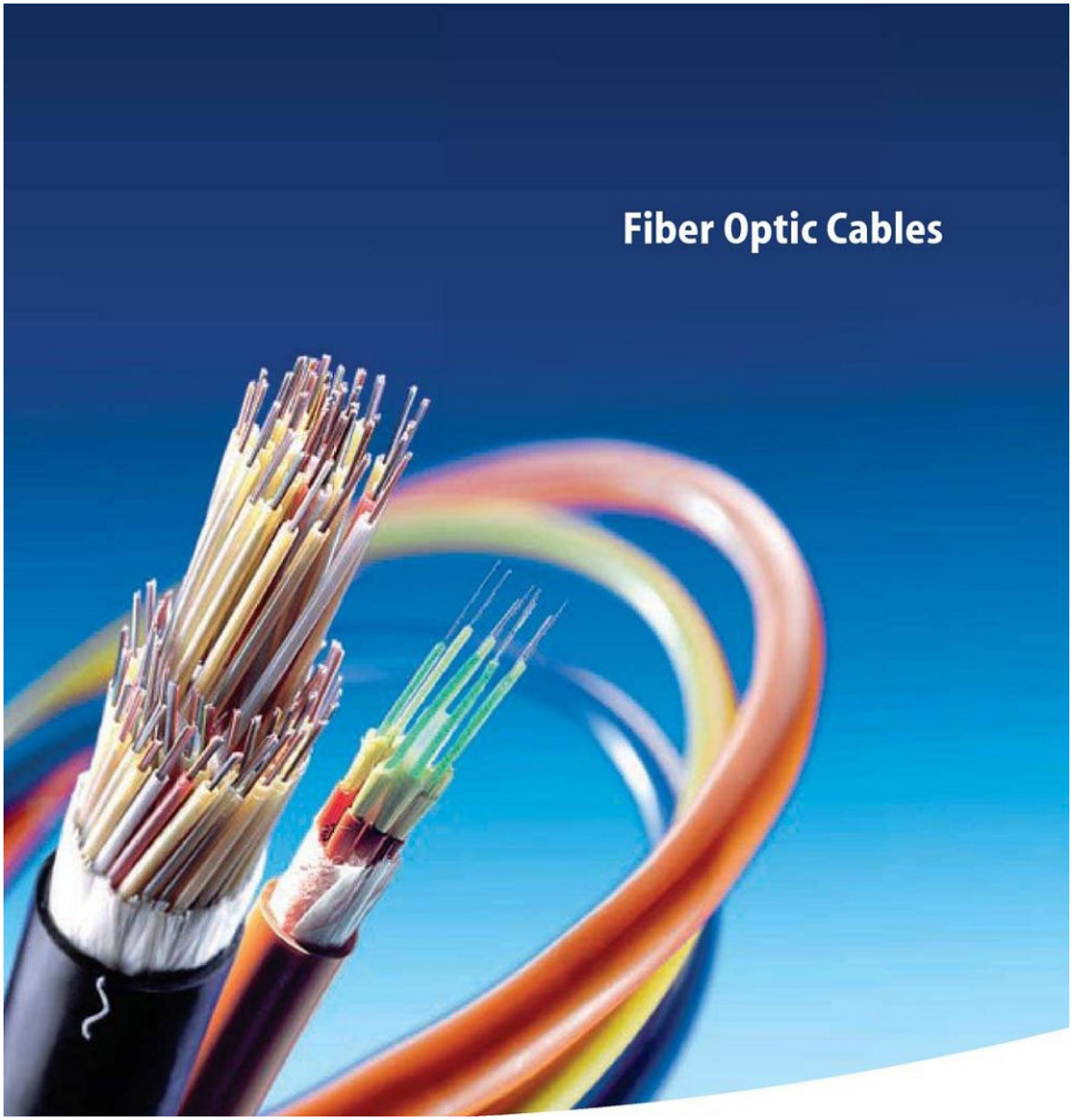
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

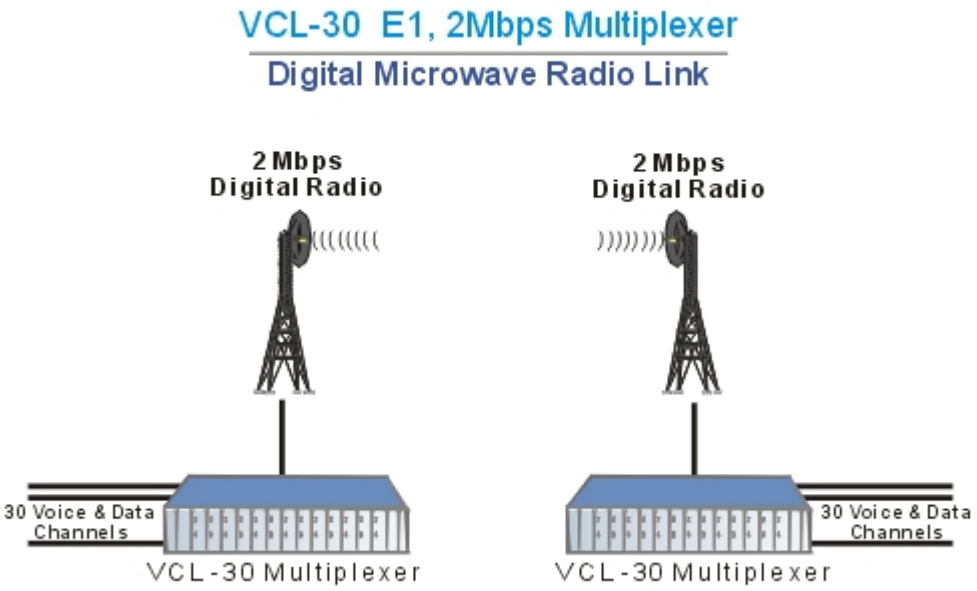
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Licensed to Berend Post berend.post@it-university.nl

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System

Radio systems are used for short distance, cheap and easy to intercept.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike

Licensed to Berend Post berend.post@it-university.nl

an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance, cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Reference:

CISA review manual 2014 page number 265

Question 1273

The MOST effective way to determine if IT is meeting business requirements is to establish:

- ☐ industry benchmarks.
- ☐ organizational goals.
- ☐ a capability model.
- ☒ key performance indicators (KPIs).

Question 1274

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 1275

During an audit of an organization's financial statements, an IS auditor finds that the IT general controls are deficient. What should the IS auditor recommend?

- ☐ Increase the compliance testing of the application controls.
- ☐ Place greater reliance on the application controls.
- ☒ Increase the substantive testing of the financial balances.
- ☐ Place greater reliance on the framework of control.

Question 1276

Which of the following would provide the MOST assurance that an application will work in a live environment?

- ☐ Walking through the programs to view the results of error processing
- ☐ Processing of test data to prove that data can be passed between individual programs
- ☐ Walking through the programs to view the results of processing copies of production data.
- ☒ Processing of valid and erroneous data in an acceptance test environment

Question 1277

Digital signatures are an effective control method for information exchange over an insecure network because they:

- ☒ enable nonrepudiation.
- ☐ are under the sole custody of the receiver.
- ☐ are constant over time.
- ☐ authenticate the user biometrically.

Question 1278

During the procurement process, which of the following would be the BEST indication that prospective vendors will meet the organization's needs?

- ☐ An account transition manager has been identified.
- ☒ Expected service levels are defined.
- ☐ The vendor's subcontractors have been identified.
- ☐ The service catalog is documented.

Licensed to Berend Post berend.post@it-university.nl

Question 1279

Which of the following answer specifies the correct sequence of levels within the Capability Maturity Model (CMM)?

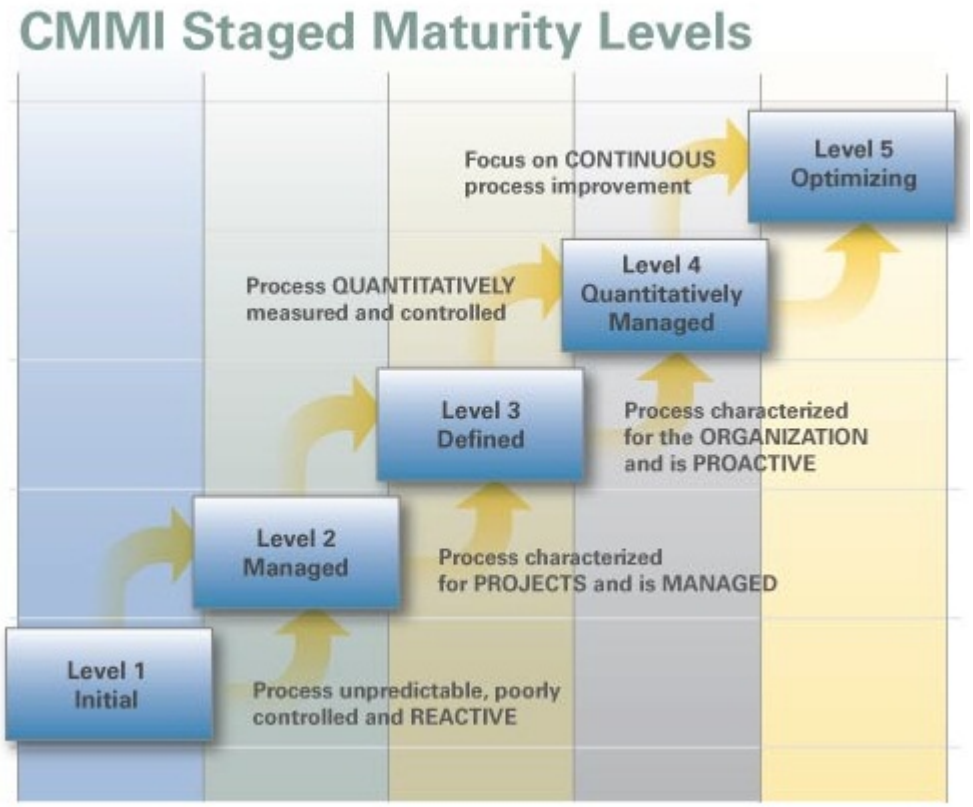
- ☒ Initial, Managed, Defined, Quantitatively managed, optimized
- ☐ Initial, Managed, Defined, optimized, Quantitatively managed
- ☐ Initial, Defined, Managed, Quantitatively managed, optimized
- ☐ Initial, Managed, Quantitatively managed, Defined, optimized

Explanation:

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.



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.

Licensed to Berend Post berend.post@it-university.nl

Structure

The model involves five aspects:

Maturity Levels: a 5-level process maturity continuum - where the uppermost (5th) level is a notional ideal state where processes would be systematically managed by a combination of process optimization and continuous process improvement.

Key Process Areas: a Key Process Area identifies a cluster of related activities that, when performed together, achieve a set of goals considered important.

Goals: the goals of a key process area summarize the states that must exist for that key process area to have been implemented in an effective and lasting way. The extent to which the goals have been accomplished is an indicator of how much capability the organization has established at that maturity level. The goals signify the scope, boundaries, and intent of each key process area.

Common Features: common features include practices that implement and institutionalize a key process area. There are five types of common features: commitment to perform, ability to perform, activities performed, measurement and analysis, and verifying implementation.

Key Practices: The key practices describe the elements of infrastructure and practice that contribute most effectively to the implementation and institutionalization of the area.

Levels

There are five levels defined along the continuum of the model and, according to the SEI: "Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief".

Initial (chaotic, ad hoc, individual heroics) - the starting point for use of a new or undocumented repeat process.

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.

Licensed to Berend Post berend.post@it-university.nl

Optimizing - process management includes deliberate process optimization/improvement.

Within each of these maturity levels are Key Process Areas which characteristic that level, and for each such area there are five factors: goals, commitment, ability, measurement, and verification. These are not necessarily unique to CMM, representing — as they do — the stages that organizations must go through on the way to becoming mature.

The model provides a theoretical continuum along which process maturity can be developed incrementally from one level to the next. Skipping levels is not allowed/feasible.

Level 1 - Initial (Chaotic)

It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place (i.e., they are the AS-IS processes) and used to establish consistency of process performance across the organization.

Level 4 - Managed

It is characteristic of processes at this level that, using process metrics, management can effectively control the AS-IS process (e.g., for software development). In particular, management can identify ways to adjust and adapt the process to particular projects without measurable losses of quality or deviations from specifications. Process Capability is established from this level.

Level 5 - Optimizing

It is a characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements.

Licensed to Berend Post berend.post@it-university.nl

At maturity level 5, processes are concerned with addressing statistical common causes of process variation and changing the process (for example, to shift the mean of the process performance) to improve process performance. This would be done at the same time as maintaining the likelihood of achieving the established quantitative process-improvement objectives.

The following answers are incorrect:

The other option specified in the option does not provide correct sequence.

Reference:

CISA review manual 2014 Page number 188

CISSP Official study guide page number 693

Question 1280

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

- ☐ dependency on a single person.
- ☐ inadequate succession planning.
- ☒ one person knowing all parts of a system.
- ☐ a disruption of operations.

Explanation:

Explanation:

Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

Question 1281

The PRIMARY benefit of a centralized time server is that it:

- ☐ reduces individual time-of-day requests by client applications
- ☐ is required by password synchronization programs
- ☒ allows decentralized logs to be kept in synchronization
- ☐ decreases the likelihood of an unrecoverable systems failure

Licensed to Berend Post berend.post@it-university.nl

Question 1282

When continuous monitoring systems are being implemented, an IS auditor should FIRST identify:

- ☐ the location and format of output files
- ☐ applications that provide the highest financial risk
- ☐ high-risk areas within the organization
- ☒ the controls on which to focus

Question 1283

Who is accountable for maintaining appropriate security measures over information assets?

- ☒ Data and systems owners
- ☐ Data and systems users
- ☐ Data and systems custodians
- ☐ Data and systems auditors

Explanation:

Explanation:

Data and systems owners are accountable for maintaining appropriate security measures over information assets.

Question 1284

A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?

- ☐ Rewrite the hard disk with random Os and Is.
- ☐ Low-level format the hard disk.
- ☐ Demagnetize the hard disk.
- ☒ Physically destroy the hard disk.

Explanation:

Explanation:

Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical, because the hard disk is damaged. Demagnetizing is an inefficient procedure, because it requires specialized and expensive equipment to be fully effective.

Licensed to Berend Post berend.post@it-university.nl

Question 1285

During an IS audit, it is discovered that security configurations differ across the organization's virtual server farm. Which of the following is the IS auditor's BEST recommendation for improving the control environment?

- ☐ Conduct an independent review of each server's security configuration
- ☒ Implement a security configuration baseline for virtual servers
- ☐ Implement security monitoring controls for high-risk virtual servers
- ☐ Conduct a standard patch management review across the virtual server farm

Question 1286

Two servers are deployed in a cluster to run a mission-critical application. To determine whether the system has been designed for optimal efficiency, the IS auditor should verify that:

- ☐ the security features in the operating system are all enabled
- ☐ the number of disks in the cluster meets minimum requirements
- ☐ the two servers are of exactly the same configuration
- ☒ load balancing between the servers has been implemented

Question 1287

An IS auditor finds that firewalls are outdated and not supported by vendors. Which of the following should be the auditor's NEXT course of action?

- ☐ Determine the value of the firewall.
- ☒ Report the security posture of the organization.
- ☐ Report the mitigating controls.
- ☐ Determine the risk of not replacing the firewall.

Question 1288

The success of an IT projects is measured PRIMARILY by the:

- ☐ translation of business vision to function vision
- ☐ implementation of current technology
- ☒ benefit that the business derives from the outcome
- ☐ efficient use of resources

Licensed to Berend Post berend.post@it-university.nl

Question 1289

An IS auditor reviewing a recently implemented virtual environment notices discrepancies among similar machine setups. Which of the following should the auditor recommend to minimize configuration risks?

- ☐ Implement network best practice recommendations
- ☐ Perform architectural vulnerability analysis to compare current system attributes to a reference
- ☐ Perform hypervisor software updates with available patches to minimize security weakness
- ☒ Implement templates to manage rapid deployment of virtual machines

Question 1290

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 1291

An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- ☐ technical platforms between the two companies are interoperable.
- ☒ parent bank is authorized to serve as a service provider.
- ☐ security features are in place to segregate subsidiary trades.
- ☐ subsidiary can join as a co-owner of this payment system.

Explanation:

Explanation:

Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as banking. Unless granted to serve as a service provider, it may not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider. The ownership of the payment system is not as important as the legal authorization to operate the system.

Licensed to Berend Post berend.post@it-university.nl

Question 1292

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 1293

The PRIMARY purpose of aligning information security with corporate governance objectives is to:

- ☐ identify an organization’s tolerance for risk.
- ☐ re-align roles and responsibilities.
- ☒ build capabilities to improve security processes.
- ☐ consistently manage significant areas of risk.

Question 1294

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1295

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 1296

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 1297

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

Licensed to Berend Post berend.post@it-university.nl

Question 1298

Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?

- ☐ Data backups are performed on a timely basis
- ☐ A recovery site is contracted for and available as needed
- ☒ Human safety procedures are in place
- ☐ insurance coverage is adequate and premiums are current

Explanation:

Explanation:

The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.

Question 1299

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

- ☐ Data
- ☒ Segment
- ☐ Packet
- ☐ Frame

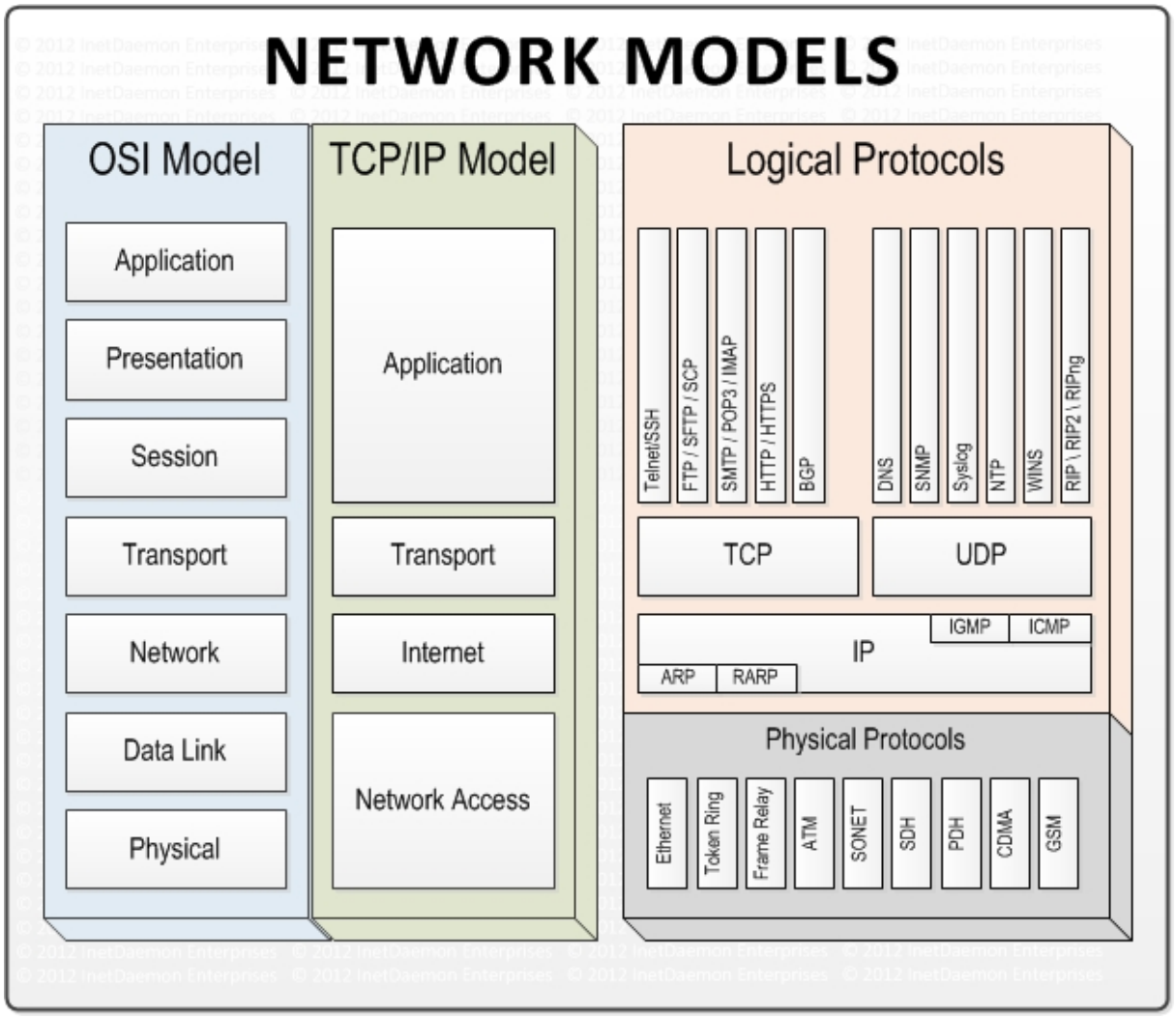
Explanation:

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.

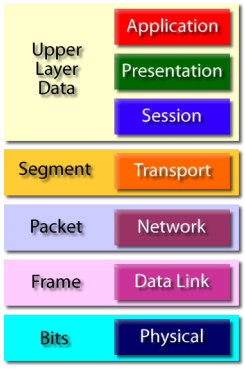
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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):



The following answers are incorrect:

Data – Application layer PDU

Packet – Network interface layer PDU

Frame/bit – LAN or WAN interface layer PDU

Reference:

CISA review manual 2014 page number 272

Question 1300

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

- ☒ allow changes, which will be completed using after-the-fact follow-up.
- ☐ allow undocumented changes directly to the production library.
- ☐ do not allow any emergency changes.
- ☐ allow programmers permanent access to production programs.

Explanation:

Explanation:

There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should be completed using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied;

Licensed to Berend Post berend.post@it-university.nl

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 1301

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 1302

The final acceptance testing of a new application system should be the responsibility of the:

- ☐ IS audit team.
- ☒ user group
- ☐ IS management
- ☐ quality assurance team

Question 1303

An audit team has a completed schedule approved by the audit committee. After starting some of the scheduled audits, executive management asked the team to immediately audit an additional process. There are not enough resources available to add the additional audit to the schedule. Which of the following is the BEST course of action?

- ☐ Revise the scope of scheduled audits.
- ☒ Propose a revised audit schedule.
- ☐ Approve overtime work to ensure the audit is completed.
- ☐ Consider scheduling the audit for the next period.

Licensed to Berend Post berend.post@it-university.nl

Question 1304

With the help of a security officer, granting access to data is the responsibility of:

- ☒ data owners.
- ☐ programmers.
- ☐ system analysts.
- ☐ librarians.

Explanation:

Explanation:

Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration with the owners' approval sets up access rules stipulating which users or group of users are authorized to access data or files and the level of authorized access (e.g., read or update).

Question 1305

How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

- ☐ By implementing redundant systems and applications onsite
- ☒ By geographically dispersing resources
- ☐ By retaining onsite data backup in fireproof vaults
- ☐ By preparing BCP and DRP documents for commonly identified disasters

Explanation:

Explanation:

Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

Question 1306

Which of the following would be an information security manager's PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?

- ☐ End user acceptance
- ☒ Mobile application control
- ☐ Configuration management
- ☐ Disparate device security

Licensed to Berend Post berend.post@it-university.nl

Question 1307

Which of the following should be established FIRST when initiating a control self-assessment program in a small organization?

- ☐ Control baselines
- ☒ Client questionnaires
- ☐ External consultants
- ☐ Facilitated workshops

Question 1308

Which of the following is a passive attack on a network?

- ☐ Message service interruption
- ☐ Message modification
- ☒ Traffic analysis
- ☐ Sequence analysis

Question 1309

What are often the primary safeguards for systems software and data?

- ☐ Administrative access controls
- ☒ Logical access controls
- ☐ Physical access controls
- ☐ Detective access controls

Explanation:

Explanation:

Logical access controls are often the primary safeguards for systems software and datA.

Question 1310

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them. zombie computers are being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☒ DDoS
- ☐ ATP
- ☐ Social Engineering
- ☐ None of the choices.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation: "Distributed denial of service (DDoS) attacks are common, where a large number of compromised hosts (""zombie computers"") are used to flood a target system with network requests, thus attempting to render it unusable through resource exhaustion."

Question 1311

Which of the following observations should be of concern to an IS auditor in the fieldwork stage of a procurement audit?

- ☒ Requisitions are being processed by the finance team.
- ☐ The purchase requester receives notifications of goods delivery.
- ☐ Purchase commitments are made prior to requisitions being approved.
- ☐ Requisitions are being facilitated by a third-party procurement service.

Question 1312

Which of the following is the MAIN purpose of an information security management system?

- ☐ To enhance the impact of reports used to monitor information security incidents
- ☒ To reduce the frequency and impact of information security incidents
- ☐ To identify and eliminate the root causes of information security incidents
- ☐ To keep information security policies and procedures up-to-date

Question 1313

Which of the following provides the MOST helpful information to determine how much data an organization can afford to lose when a critical system failure occurs?

- ☐ Industry data loss statistics
- ☐ Risk assessment results
- ☒ Recovery point objective (RPO)
- ☐ Recovery time objective (RTO)

Question 1314

At the completion of a system development project, a post project review should include which of the following?

- ☐ Assessing risks that may lead to downtime after the production release
- ☒ Identifying lessons learned that may be applicable to future projects
- ☐ Verifying the controls in the delivered system are working
- ☐ Ensuring that test data are deleted

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment of potential downtime should be made with the operations group and other specialists before implementing a system. Verifying that controls are working should be covered during the acceptance test phase and possibly, again, in the post implementation review. Test data should be retained for future regression testing.

Question 1315

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 1316

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 1317

During a help desk review, an IS auditor determines the call abandonment rate exceeds agreed-upon service levels. What conclusions can be drawn from this finding?

- ☐ There are insufficient telephone lines available to the help desk.
- ☒ There is insufficient staff to handle the help desk call volume.
- ☐ Help desk staff are unable to resolve a sufficient number of problems on the first call.
- ☐ Users are finding solutions from alternative sources.

Question 1318

Which of the following would BEST assist senior management in evaluating IT performance as well as the alignment between corporate and IT strategic objectives?

- ☐ Enterprise architecture (EA)
- ☐ IT project value analysis
- ☒ Balanced scorecard
- ☐ Control self-assessment (CSA)

Question 1319

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 1320

Which function in the purchasing module of an enterprise resource planning (ERP) system ensures payments are not issued for incorrect invoices?

- ☐ Sequential payment numbers
- ☒ Three-way match
- ☐ Purchasing authority levels
- ☐ Management workflow approval

Licensed to Berend Post berend.post@it-university.nl

Question 1321

Malicious program code was found in an application and corrected prior to release into production. After the release, the same issue was reported. Which of the following is the IS auditor's BEST recommendation?

- ☐ Ensure the business signs off on end-to-end user acceptance test results.
- ☒ Ensure corrected program code is compiled in a dedicated server.
- ☐ Ensure change management reports are independently reviewed.
- ☐ Ensure programmers cannot access code after the completion of program edits.

Question 1322

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 1323

Which of the following is the MOST effective way to assess whether an outsourcer's controls are following the service level agreement (SLA)?

- ☒ Perform an onsite review of the outsourcer.
- ☐ Review the outsourcer's monthly service reports.
- ☐ Perform a review of penalty clauses for non-performance.
- ☐ Review an internal audit report from the outsourcer's auditor.

Licensed to Berend Post berend.post@it-university.nl

Question 1324

A security company and service provider have merged, and the CEO has requested one comprehensive set of security policies be developed for the newly formed company. The IS auditor's BEST recommendation would be to:

- ☒ conduct a policy gap assessment.
- ☐ adopt an industry standard security policy.
- ☐ implement the service provider's policies.
- ☐ implement the security company's policies.

Question 1325

A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

- ☒ Issues of privacy
- ☐ Wavelength can be absorbed by the human body
- ☐ RFID tags may not be removable
- ☐ RFID eliminates line-of-sight reading

Explanation:

Explanation:

The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

Question 1326

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1327

Due to a recent business divesture, an organization has limited IT resources to deliver critical projects. Reviewing the IT staffing plan against which of the following would BEST guide IT management when estimating resource requirements for future projects?

- ☐ Peer organizational staffing benchmarks
- ☐ Budgeted forecast for the next financial year
- ☒ Human resources sourcing strategy
- ☐ Records of actual time spent on projects

Question 1328

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:

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.

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.

Reference:

CISA review manual 2014 page number 266

Licensed to Berend Post berend.post@it-university.nl

Question 1329

Which of the following is of greatest concern when performing an IS audit?

- ☒ Users' ability to directly modify the database
- ☐ Users' ability to submit queries to the database
- ☐ Users' ability to indirectly modify the database
- ☐ Users' ability to directly view the database

Explanation:

Explanation:

A major IS audit concern is users' ability to directly modify the database.

Question 1330

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:

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.

Licensed to Berend Post berend.post@it-university.nl

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.

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.

Reference:

CISA review manual 2014 Page number 352

Question 1331

While observing a full simulation of the business continuity plan, an IS auditor notices that the notification systems within the organizational facilities could be severely impacted by infra structural damage. The BEST recommendation the IS auditor can provide to the organization is to ensure:

- ☐ the salvage team is trained to use the notification system.
- ☐ the notification system provides for the recovery of the backup.
- ☒ redundancies are built into the notification system.
- ☐ the notification systems are stored in a vault.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

If the notification system has been severely impacted by the damage, redundancy would be the best control. The salvage team would not be able to use a severely damaged notification system, even if they are trained to use it. The recovery of the backups has no bearing on the notification system and storing the notification system in a vault would be of little value if the building is damaged.

Question 1332

Audit software designed to detect invalid data, extreme values, or linear correlations between data elements can be classified as which type of data analytics tool?

- ☐ Descriptive
- ☒ Diagnostic
- ☐ Predictive
- ☐ Prescriptive

Question 1333

Which of the following layer of the OSI model provides a standard interface for applications to communicate with devices on a network?

- ☒ Application layer
- ☐ Presentation layer
- ☐ Session layer
- ☐ Transport layer

Explanation:

Explanation:

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

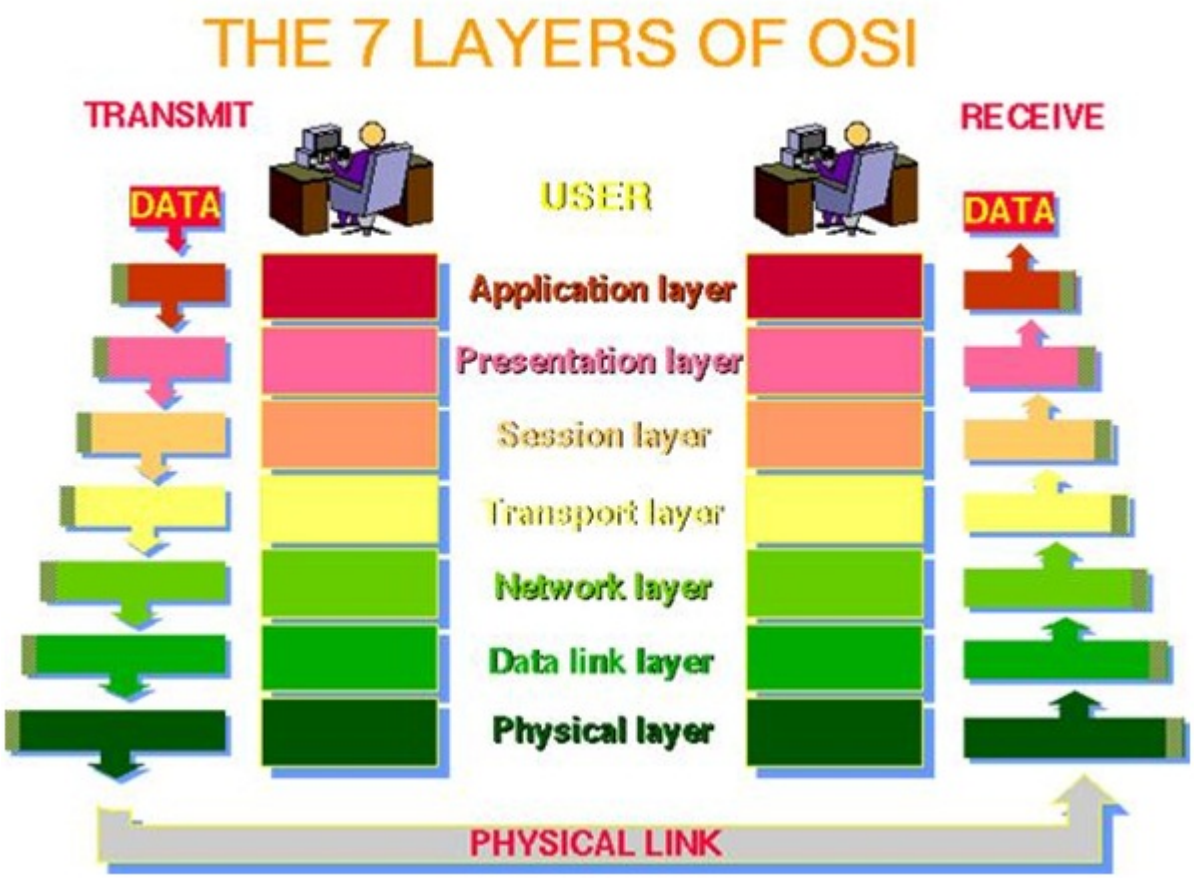
Licensed to Berend Post berend.post@it-university.nl

For your exam you should know below information about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model



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

Licensed to Berend Post berend.post@it-university.nl

electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1

How the receiving station knows when a "bit-time" starts

How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

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.

Licensed to Berend Post berend.post@it-university.nl

Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

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).

Licensed to Berend Post berend.post@it-university.nl

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, pretending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER

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.

Licensed to Berend Post berend.post@it-university.nl

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection

Remote file access

Remote printer access

Inter-process communication

Network management

Directory services

Electronic messaging (such as mail)

Network virtual terminals

The following were incorrect answers:

Presentation layer - The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

Session layer - The session layer allows session establishment between processes running on different stations.

Transport layer - The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

Reference:

CISA review manual 2014 Page number 260

Licensed to Berend Post berend.post@it-university.nl

Question 1334

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 1335

When auditing the security architecture of an e-commerce environment, an IS auditor should FIRST review the:

- ☒ configuration of the firewall
- ☐ alternate firewall arrangements
- ☐ location of the firewall within the network
- ☐ criteria used for selecting the firewall

Licensed to Berend Post berend.post@it-university.nl

Question 1336

An organization is considering outsourcing the processing of customer insurance claims. An IS auditor notes that customer data will be sent offshore for processing. Which of the following would be the BEST way to address the risk of exposing customer data?

- ☐ Require background checks on all service provider personnel involved in the processing of data.
- ☐ Recommend the use of a service provider within the same country as the organization.
- ☐ Consider whether the service provider has the ability to meet service level agreements (SLAs).
- ☒ Assess whether the service provider meets the organization's data protection policies.

Question 1337

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 1338

Which of the following is MOST likely to improve the portability of an application connected to a database?

- ☐ Analyzing stored procedures and triggers
- ☒ Optimizing the database physical schema
- ☐ Verifying database import and export procedures
- ☐ Using a structured query language (SQL)

Licensed to Berend Post berend.post@it-university.nl

Question 1339

Which of the following is the BEST indication that an organization has achieved legal and regulatory compliance?

- ☐ The board of directors and senior management accept responsibility for compliance.
- ☐ An independent consultant has been appointed to ensure legal and regulatory compliance.
- ☒ Periodic external and internal audits have not identified instances of noncompliance.
- ☐ The risk management process incorporates noncompliance as a risk.

Question 1340

Which of the following tools are MOST helpful for benchmarking an existing IT capability?

- ☐ Prior IS audit reports
- ☐ IT maturity models
- ☐ Risk assessments
- ☒ IT balanced scorecards

Question 1341

Which of the following attack redirects outgoing message from the client back onto the client, preventing outside access as well as flooding the client with the sent packets?

- ☒ Banana attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Explanation:

Explanation:

A "banana attack" is another particular type of DoS. It involves redirecting outgoing messages from the client back onto the client, preventing outside access, as well as flooding the client with the sent packets.

The Banana attack uses a router to change the destination address of a frame. In the Banana attack:

A compromised router copies the source address on an inbound frame into the destination address.

The outbound frame bounces back to the sender.

This sender is flooded with frames and consumes so many resources that valid service requests can no longer be processed.

Licensed to Berend Post berend.post@it-university.nl

The following answers are incorrect:

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Reference:

CISA review manual 2014 Page number 321

Question 1342

Which of the following is the MOST important role of the information security manager when the organization is in the process of adopting emerging technologies?

- ☒ Understanding the impact on existing resources
- ☐ Assessing how peer organizations using the same technologies have been impacted
- ☐ Developing training for end users to familiarize them with the new technology
- ☐ Reviewing vendor documentation and service levels agreements

Question 1343

Which of the following is the MOST effective way to verify an organization’s ability to continue its essential business operations after a disruption event? Analysis of:

- ☐ end-to-end recovery flow
- ☐ recovery point objectives (RPOs)
- ☐ call trees
- ☒ business impact analysis (BIA)

Licensed to Berend Post berend.post@it-university.nl

Question 1344

During the system testing phase of an application development project the IS auditor should review the:

- ☐ conceptual design specifications.
- ☐ vendor contract.
- ☒ error reports.
- ☐ program change requests.

Explanation:

Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

Question 1345

In which of the following cloud service models does the user organization have the GREATEST control over the accuracy of configuration items in its configuration management database (CMDB)?

- ☐ Database as a Service (DbaaS)
- ☐ Software as a Service (SaaS)
- ☐ Platform as a Service (PaaS)
- ☒ Infrastructure as a Service (IaaS)

Question 1346

Which of the following is the BEST way to help ensure the security of privacy-related data stored by an organization?

- ☒ Encrypt personally identifiable information (PII).
- ☐ Publish the data classification scheme.
- ☐ Inform data owners of the purpose of collecting information.
- ☐ Classify privacy-related data as confidential.

Licensed to Berend Post berend.post@it-university.nl

Question 1347

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 1348

A start-up organization wants to develop a data loss prevention program (DLP). The FIRST step should be to implement:

- ☐ data encryption.
- ☐ access controls.
- ☒ data classification.
- ☐ security awareness training.

Question 1349

Who provides the funding to the project and works closely with the project manager to define critical success factor (CSF)?

- ☒ Project Sponsor
- ☐ Security Officer
- ☐ User Management
- ☐ Senior Management

Explanation:

Explanation:

Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

For the CISA exam you should know the information below about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

Licensed to Berend Post berend.post@it-university.nl

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?

How reliable is the software?

How effective is the software?

Is the software easy to use?

How easy is to transfer or adapt old data from preexisting software to this environment?

Is it possible to add new functions?

Does it meet regulatory requirement?

Project Steering Committee – Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

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.

Licensed to Berend Post berend.post@it-university.nl

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:

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

Reference:

CISA review manual 2014 Page number 150

Licensed to Berend Post berend.post@it-university.nl

Question 1350

Which of the following would BEST detect logic bombs in the new programs?

- ☐ Final acceptance testing by users
- ☐ Parallel/pilot testing
- ☒ Regression testing
- ☐ Independent program review

Question 1351

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.

Question 1352

Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?

- ☐ There are three individuals with a key to enter the area.
- ☐ Paper documents are also stored in the offsite vault.
- ☒ Data files that are stored in the vault are synchronized.
- ☐ The offsite vault is located in a separate facility.

Explanation:

Explanation:

Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

Licensed to Berend Post berend.post@it-university.nl

Question 1353

The sender of a public key would be authenticated by a:

- ☐ certificate authority,
- ☐ digital signature.
- ☒ digital certificate.
- ☐ registration authority.

Explanation:

Explanation:

A digital certificate is an electronic document that declares a public key holder is who the holder claims to be. The certificates do handle data authentication as they are used to determine who sent a particular message. A certificate authority issues the digital certificates, and distributes, generates and manages public keys. A digital signature is used to ensure integrity of the message being sent and solve the nonrepudiation issue of message origination. The registration authority would perform most of the administrative tasks of a certificate authority, i.e., registration of the users of a digital signature plus authenticating the information that is put in the digital certificate.

Question 1354

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 1355

A recent audit identified duplicate software licenses and technologies. Which of the following would be MOST helpful to prevent this type of duplication in the future?

- ☐ Centralizing IT procurement and approval practices
- ☒ Updating IT procurement policies and procedures
- ☐ Conducting periodic inventory reviews
- ☐ Establishing a project management office

Licensed to Berend Post berend.post@it-university.nl

Question 1356

During an audit, which of the following would be MOST helpful in establishing a baseline for measuring data quality?

- ☐ Built-in data error prevention application controls
- ☐ Industry standard business definitions
- ☐ Input from customers
- ☒ Validation of rules by the business

Question 1357

In a small organization, an IS auditor finds that security administration and system analysis functions are performed by the same employee. Which of the following is the MOST significant finding?

- ☐ The security policy has not been updated to reflect the situation.
- ☐ The employee's formal job description has not been updated.
- ☐ The employee has not signed the security policy.
- ☒ The employee's activities are not independently reviewed.

Question 1358

Which of the following is the BEST approach to verify that internal help desk procedures are executed in compliance with policies?

- ☐ Benchmark help desk procedures.
- ☐ Interview end users.
- ☒ Test a sample of closed tickets.
- ☐ Evaluate help desk call metrics.

Question 1359

Which of the following is the MOST important prerequisite for implementing a data loss prevention (DLP) tool?

- ☐ Identifying where existing data resides and establishing a data classification matrix.
- ☐ Requiring users to save files in secured folders instead of a company-wide shared drive
- ☐ Reviewing data transfer logs to determine historical patterns of data flow
- ☒ Developing a DLP policy and requiring signed acknowledgement by users

Licensed to Berend Post berend.post@it-university.nl

Question 1360

An IS auditor is reviewing an organization's method to transport sensitive data between offices. Which of the following would cause the auditor MOST concern?

- ☐ The method relies exclusively on the use of digital signatures.
- ☐ The method relies exclusively on the use of asymmetric encryption algorithms.
- ☐ The method relies exclusively on the use of public key infrastructure.
- ☒ The method relies exclusively on the use of symmetric encryption algorithms.

Question 1361

Which of the following is the MOST important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings?

- ☐ Peak activity periods for the business
- ☒ Remediation dates included in management responses
- ☐ Availability of IS audit resources
- ☐ Complexity of business processes identified in the audit

Question 1362

Which of the following is an oft-cited cause of vulnerability of networks?

- ☒ software monoculture
- ☐ software diversification
- ☐ single line of defense
- ☐ multiple DMZ
- ☐ None of the choices.

Explanation:

Explanation:

An oft-cited cause of vulnerability of networks is homogeneity or software monoculture. In particular, Microsoft Windows has such a large share of the market that concentrating on it will enable a cracker to subvert a large number of systems. Introducing inhomogeneity purely for the sake of robustness would however bring high costs in terms of training and maintenance.

Question 1363

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:

Licensed to Berend Post berend.post@it-university.nl

The primary purpose of digital signatures is to provide authentication and integrity of data.

Question 1364

An IS auditor begins an assignment and identifies audit components for which the auditor is not qualified to assess. Which of the following is the BEST course of action?

- ☒ Notify audit management for a decision on how to proceed.
- ☐ Complete the audit and give full disclosure in the final audit report.
- ☐ Complete the work assignment to the best of the auditor's ability.
- ☐ Exclude the related tests from the audit plan and continue the assignment.

Question 1365

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 1366

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

- ☐ Signature-based
- ☒ Neural networks-based
- ☐ Statistical-based
- ☐ Host-based

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning. Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

Question 1367

Which of the following is the MOST important consideration when deploying closed-circuit television (CCTV) systems that use wireless communication links to transmit images between cameras and a receiver?

- ☐ Encryption of transmissions
- ☒ Monitoring by security guards
- ☐ Retention period of recordings
- ☐ Strategic placement of cameras

Question 1368

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 1369

When protecting an organization's IT systems, which of the following is normally the next line of defense after the network firewall has been compromised?

- ☐ Personal firewall
- ☐ Antivirus programs
- ☒ Intrusion detection system (IDS)
- ☐ Virtual local area network (VLAN) configuration

Explanation:

Explanation:

An intrusion detection system (IDS) would be the next line of defense after the firewall. It would detect anomalies in the network/server activity and try to detect the perpetrator. Antivirus programs, personal firewalls and VIAN configurations would be later in the line of defense.

Licensed to Berend Post berend.post@it-university.nl

Question 1370

The reliability of an application system's audit trail may be questionable if:

- ☐ user IDs are recorded in the audit trail.
- ☐ the security administrator has read-only rights to the audit file.
- ☐ date and time stamps are recorded when an action occurs.
- ☒ users can amend audit trail records when correcting system errors.

Explanation:

Explanation:

An audit trail is not effective if the details in it can be amended.

Question 1371

Which of the following is MOST helpful when establishing the authenticity of digital evidence collected from a hard disk?

- ☒ Bit-by-bit image of the hard disk
- ☐ Hash of the files on the hard disk
- ☐ Chain of custody documentation
- ☐ Confirmation by witnesses

Question 1372

Which of the following should be the PRIMARY basis for planning and prioritizing IT infrastructure security audits?

- ☒ Asset value to the organization
- ☐ Management requests
- ☐ The organization's risk appetite
- ☐ Security best practice

Question 1373

An IS auditor reviews change control tickets and finds an emergency change request where an IT manager approved the change, modified the code on the production platform, and resolved the ticket. Which of the following should be the auditor's GREATEST concern?

- ☒ There was no follow-up approval from the business.
- ☐ The change was made less than an hour after the request.
- ☐ There was no testing prior to making the change in production.
- ☐ The IT manager performed the change and resolved the ticket.

Licensed to Berend Post berend.post@it-university.nl

Question 1374

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 1375

Which of the following controls is MOST appropriate against brute force attacks at login?

- ☐ Storing password files using one-way encryption
- ☒ Locking the account after three invalid passwords
- ☐ Storing passwords under a one-way hash function
- ☐ Increasing the minimum password length to 10 characters

Question 1376

What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

- ☐ Accuracy check
- ☐ Completeness check
- ☒ Reasonableness check
- ☐ Redundancy check

Explanation:

Explanation:

A reasonableness check is a data validation edit control that matches input data to an occurrence rate.

Question 1377

Which of the following is the MOST important advantage of participating in beta testing of software products?

- ☐ It improves vendor support and training.
- ☒ It enables an organization to gain familiarity with new products and their functionality.
- ☐ It increases an organization's ability to retain staff who prefer to work with new technology.
- ☐ It enhances security and confidentiality.

Licensed to Berend Post berend.post@it-university.nl

Question 1378

Audit management has just completed the annual audit plan for the upcoming year, which consists entirely of high-risk processes. However, it is determined that there are insufficient resources to execute the plan. What should be done NEXT?

- ☐ Remove audits from the annual plan to better match the number of resources available
- ☐ Reduce the scope of the audits to better match the number of resources available
- ☒ Present the annual plan to the audit committee and ask for more resources
- ☐ Review the audit plan and defer some audits to the subsequent year

Question 1379

The goal of an information system is to achieve integrity, authenticity and non-repudiation of information's sent across the network. Which of the following statement correctly describe the steps to address all three?

- ☐ Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message.
- ☐ Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key.
- ☐ Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key.
- ☒ Encrypt message digest using sender's private key and then send the encrypted digest to the receiver along with original message. Receiver can decrypt the same using sender's public key.

Explanation:

Explanation:

The digital signature is used to achieve integrity, authenticity and non-repudiation. In a digital signature, the sender's private key is used to encrypt the message digest of the message. Encrypting the message digest is the act of Signing the message. The receiver will use the matching public key of the sender to decrypt the Digital Signature using the sender's public key.

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures cannot be forged by someone else who does not possess the private key, it can also be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital

Licensed to Berend Post berend.post@it-university.nl

certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real and has not been modified since the day it was issued.

How Digital Signature Works

Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you.

You copy-and-paste the contract (it's a short one!) into an e-mail note.

Using special software, you obtain a message hash (mathematical summary) of the contract.

You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.

The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

To make sure it's intact and from you, your lawyer makes a hash of the received message.

Your lawyer then uses your public key to decrypt the message hash or summary.

If the hashes match, the received message is valid.

Below are some common reasons for applying a digital signature to communications:

Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. The importance of high assurance in the sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a serious mistake.

Integrity

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it.(Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a

 Licensed to Berend Post berend.post@it-university.nl

message is digitally signed, any change in the message after the signature has been applied would invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that authentication, non-repudiation, and other properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability, else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". This is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen.

Tip for the exam

Digital Signature does not provide confidentiality. It provides only authenticity and integrity. The sender's private key is used to encrypt the message digest to calculate the digital signature

Encryption provides only confidentiality. The receiver's public key or symmetric key is used for encryption

The following were incorrect answers:

Encrypt the message digest using symmetric key and then send the encrypted digest to receiver along with original message - Symmetric key encryption does not provide non-repudiation as symmetric key is shared between users

Encrypt the message digest using receiver's public key and then send the encrypted digest to receiver along with original message. The receiver can decrypt the message digest using his own private key - Receiver's public key is known to everyone. This will not address non-repudiation

Encrypt the message digest using sender's public key and then send the encrypted digest to the receiver along with original message. The receiver can decrypt using his own private key -The sender public key is known to everyone. If sender's key is used for encryption, then sender's private key is

 Licensed to Berend Post berend.post@it-university.nl

required to decrypt data. The receiver will not be able to decrypt the digest as receiver will not have sender's private key.

Reference:

CISA review manual 2014 Page number 331

http://upload.wikimedia.org/wikipedia/commons/2/2b/Digital_Signature_diagram.svg

http://en.wikipedia.org/wiki/Digital_signature

http://searchsecurity.techtarget.com/definition/digital-signature

Question 1380

An IS auditor reviewing security incident processes realizes incidents are resolved and closed, but root causes are not investigated. Which of the following should be the MAJOR concern with this situation?

- ☒ Abuses by employees have not been reported.
- ☐ Vulnerabilities have not been properly addressed.
- ☐ Security incident policies are out of date.
- ☐ Lessons learned have not been properly documented.

Question 1381

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1382

The PRIMARY objective of value delivery in reference to IT governance is to:

- ☐ increase efficiency
- ☐ promote best practices
- ☒ optimize investments
- ☐ ensure compliance

Question 1383

Which of the following append themselves to files as a protection against viruses?

- ☐ Behavior blockers
- ☐ Cyclical redundancy checkers (CRCs)
- ☒ Immunizers
- ☐ Active monitors

Explanation:

Explanation:

Immunizers defend against viruses by appending sections of themselves to files. They continuously check the file for changes and report changes as possible viral behavior. Behavior blockers focus on detecting potentially abnormal behavior, such as writing to the boot sector or the master boot record, or making changes to executable files. Cyclical redundancy checkers compute a binary number on a known virus-free program that is then stored in a database file. When that program is subsequently called to be executed, the checkers look for changes to the files, compare it to the database and report possible infection if changes have occurred. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions.

Question 1384

While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered. Which of the following control is implemented by Lily?

- ☐ Range Check
- ☒ Duplicate Check
- ☐ Existence check
- ☐ Reasonableness check

Explanation:

Explanation:

In a duplicate check control new transaction are matched to those previously input to ensure that they have not already been entered. For ex. A vendor invoice number agrees with previously recorded invoice to ensure that the current order is not a duplicate and, therefore, the vendor will not be paid twice.

Licensed to Berend Post berend.post@it-university.nl

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.

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

 Licensed to Berend Post berend.post@it-university.nl

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.

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.

Reference:

CISA review manual 2014 Page number 215

Licensed to Berend Post berend.post@it-university.nl

Question 1385

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 1386

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- ☐ implementation.
- ☐ compliance.
- ☐ documentation.
- ☒ sufficiency.

Explanation:

Explanation:

An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

Question 1387

Which of the following BEST enables staff acceptance of information security policies?

- ☒ Strong senior management support
- ☐ Adequate security funding
- ☐ Computer-based training
- ☐ A robust incident response program

Question 1388

An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

- ☐ Run a low-level data wipe utility on all hard drives
- ☐ Erase all data file directories
- ☐ Format all hard drives
- ☒ Physical destruction of the hard drive

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The most effective method is physical destruction. Running a low-level data wipe utility may leave some residual data that could be recovered; erasing data directories and formatting hard drives are easily reversed, exposing all data on the drive to unauthorized individuals.

Question 1389

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 1390

Which should be reviewed FIRST by an IS auditor to ensure that data is being secured appropriately for an application?

- ☒ Data classification
- ☐ Data encryption
- ☐ Data access
- ☐ Data storage

Explanation:

Explanation:

Data classification is necessary to provide proper access rights to the users. If you do not classify data according to their sensitivity and importance to the business, you cannot apply proper access rules to them. Data owners are responsible for defining access rules. The data classification process starts with the process of establishing ownership of data. This process also helps to prepare data dictionary

Question 1391

Which of the following ACID property in DBMS ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other?

- ☐ Atomicity
- ☐ Consistency
- ☒ Isolation
- ☐ Durability

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other.

For CISA exam you should know below information about ACID properties in DBMS:

Atomicity - Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged. An atomic system must guarantee atomicity in each and every situation, including power failures, errors, and crashes. To the outside world, a committed transaction appears (by its effects on the database) to be indivisible ("atomic"), and an aborted transaction does not happen.

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Isolation - The isolation property ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other. Providing isolation is the main goal of concurrency control. Depending on concurrency control method, the effects of an incomplete transaction might not even be visible to another transaction. [citation needed]

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors. In a relational database, for instance, once a group of SQL statements execute, the results need to be stored permanently (even if the database crashes immediately thereafter). To defend against power loss, transactions (or their effects) must be recorded in a non-volatile memory.

The following were incorrect answers:

Consistency - The consistency property ensures that any transaction will bring the database from one valid state to another. Any data written to the database must be valid according to all defined rules, including but not limited to constraints, cascades, triggers, and any combination thereof. This does not guarantee correctness of the transaction in all ways the application programmer might have wanted (that is the responsibility of application-level code) but merely that any programming errors do not violate any defined rules.

Licensed to Berend Post berend.post@it-university.nl

Durability - Durability means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors.

Atomicity requires that each transaction is "all or nothing": if one part of the transaction fails, the entire transaction fails, and the database state is left unchanged.

Reference:

CISA review manual 2014 Page number 218

Question 1392

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 1393

An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

- ☐ Program evaluation review technique (PERT)
- ☐ Counting source lines of code (SLOC)
- ☒ Function point analysis
- ☐ White box testing

Explanation:

Explanation:

Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications. PERT is a project management technique that helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

Licensed to Berend Post berend.post@it-university.nl

Question 1394

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 1395

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 1396

Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

- ☒ Developments may result in hardware and software incompatibility.
- ☐ Resources may not be available when needed.
- ☐ The recovery plan cannot be tested.
- ☐ The security infrastructures in each company may be different.

Explanation:

Explanation:

If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based walkthroughs, and possibly by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

Licensed to Berend Post berend.post@it-university.nl

Question 1397

Which of the following is MOST important for an IS auditor to consider when reviewing the effectiveness of an incident response program?

- ☐ Incidents are categorized according to industry standards.
- ☒ Lessons learned are incorporated into incident response processes.
- ☐ Incidents are escalated to senior management in a timely manner.
- ☐ The plan is reviewed and updated annually.

Question 1398

Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?

- ☒ exploit
- ☐ patch
- ☐ quick fix
- ☐ service pack
- ☐ malware
- ☐ None of the choices.

Explanation:

Explanation:

"The term ""exploit"" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in a certain programs processing of a specific file type, such as a non-executable media file."

Question 1399

Overall business risk for a particular threat can be expressed as:

- ☒ a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
- ☐ the magnitude of the impact should a threat source successfully exploit the vulnerability.
- ☐ the likelihood of a given threat source exploiting a given vulnerability.
- ☐ the collective judgment of the risk assessment team.

Explanation:

Explanation:

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset.

Licensed to Berend Post berend.post@it-university.nl

Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

Question 1400

An organization has purchased a security information and event management (SIEM) tool. Which of the following would be MOST important to consider before implementation?

- ☐ The contract with the SIEM vendor
- ☒ Controls to be monitored
- ☐ Available technical support
- ☐ Reporting capabilities

Question 1401

An IS auditor is assessing a recent migration of mission critical applications to a virtual platform. Which of the following observations poses the GREATEST risk to the organization?

- ☐ A post-implementation review of the hypervisor has not yet been conducted.
- ☐ Role descriptions do not accurately reflect new virtualization responsibilities.
- ☐ The migration was not approved by the board of directors.
- ☒ Training for staff with new virtualization responsibilities has not been conducted.

Question 1402

Which of the following is the PRIMARY benefit of using an integrated audit approach?

- ☐ Higher acceptance of the findings from the audited business areas
- ☐ The avoidance of duplicated work and redundant recommendations
- ☐ Enhanced allocation of resources and reduced audit costs
- ☒ A holistic perspective of overall risk and a better understanding of controls

Question 1403

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

Licensed to Berend Post berend.post@it-university.nl

permission can override the write protection. Writing a duplicate log to another server or daily printing of the system log cannot prevent unauthorized changes.

Question 1404

An IS audit reveals that an organization is not proactively addressing known vulnerabilities. Which of the following should the IS auditor recommend the organization do FIRST?

- ☐ Verify the disaster recovery plan (DRP) has been tested.
- ☐ Ensure the intrusion prevention system (IPS) is effective.
- ☐ Confirm the incident response team understands the issue.
- ☒ Assess the security risks to the business.

Question 1405

Which of the following would BEST support 24/7 availability?

- ☐ Daily backup
- ☐ offsite storage
- ☒ Mirroring
- ☐ Periodic testing

Explanation:

Explanation:

Mirroring of critical elements is a too! that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not of themselves support continuous availability.

Question 1406

An IS auditor is conducting a follow-up internal IS audit and determines that several recommendations from the prior year have not been implemented. Which of the following should be the auditor's FIRST course of action?

- ☐ Evaluate the recommendations in context of the current IT environment.
- ☐ Continue the audit and disregard prior audit recommendations.
- ☐ Request management implement recommendations from the prior year.
- ☒ Add unimplemented recommendations as findings for the new audit.

Licensed to Berend Post berend.post@it-university.nl

Question 1407

The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

- ☒ Reliability and quality of service (QoS)
- ☐ Means of authentication
- ☐ Privacy of voice transmissions
- ☐ Confidentiality of data transmissions

Explanation:

Explanation:

The company currently has a VPN; issues such as authentication and confidentiality have been implemented by the VPN using tunneling. Privacy of voice transmissions is provided by the VPN protocol. Reliability and QoS are, therefore, the primary considerations to be addressed.

Question 1408

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 1409

Which of the following test approaches would utilize data analytics to test a dual approval payment control?

- ☒ Review payments completed in the past month that do not have a unique approver.
- ☐ Attempt to complete a payment without a secondary approval.
- ☐ Review users within the payment application who are assigned an approver role.
- ☐ Evaluate configuration settings for the secondary approval requirements.

Question 1410

Documentation of workaround processes to keep a business function operational during recovery of IT systems is a core part of a:

- ☐ business impact analysis (BIA).
- ☐ threat and risk assessment.
- ☒ business continuity plan (BCP).
- ☐ disaster recovery plan (DRP).

Licensed to Berend Post berend.post@it-university.nl

Question 1411

During Involuntary termination of an employee, which of the following is the MOST important step to be considered?

- ☐ Get a written NDA agreement from an employee
- ☒ Terminate all physical and logical access
- ☐ Provide compensation in lieu of notice period
- ☐ Do not communicate to the respective employee about the termination

Explanation:

Explanation:

For CISA exam you should know below information about Terminated Employee Access

Termination of employment can occur in the following circumstances:

On the request of the employee (Voluntary resignation from service)

Scheduled (On retirement or completion of contract)

Involuntary (forced by management in special circumstances)

In case of an involuntary termination of employment, the logical and physical access rights of employees to the IT infrastructure should either be withdrawn completely or highly restricted as early as possible, before the employee become aware of termination or its likelihood.

This ensures that terminated employees cannot continue to access potentially confidential or damaging information from the IT resources or perform any action that would result in damage of any kind of IT infrastructure, applications and data. Similar procedure in place to terminate access for third parties upon terminating their activities with the organization.

When it is necessary for employee to continue to have accesses, such access must be monitored carefully and continuously and should take place with senior management's knowledge and authorization.

In case of a voluntary or scheduled termination of employment, it is management's prerogative to decide whether access is restricted or withdrawn. This depends on:

The specific circumstances associated with each case

The sensitivity of employee's access to the IT infrastructure and resources

Licensed to Berend Post berend.post@it-university.nl

The requirement of the organization's information security policies, standards and procedure.

The following were incorrect answers:

The other options presented are incorrectly describes about involuntary termination.

Reference:

CISA review manual 2014 Page number 361 and 362

Question 1412

Which of the following should be an IS auditor's FIRST action when assessing the risk associated with unstructured data?

- ☐ Implement strong encryption for unstructured data.
- ☐ Implement user access controls to unstructured data.
- ☐ Identify repositories of unstructured data.
- ☒ Identify appropriate tools for data classification.

Question 1413

Which of the following mechanisms for process improvement involves examination of industry best practice?

- ☐ Continuous improvement
- ☐ Knowledge management
- ☐ Business process reengineering (BPR)
- ☒ Benchmarking

Question 1414

Which of the following would BEST facilitate the successful implementation of an IT-related framework?

- ☐ Aligning the framework to industry best practices
- ☒ Involving appropriate business representation within the framework
- ☐ Establishing committees to support and oversee framework activities
- ☐ Documenting IT-related policies and procedures

Licensed to Berend Post berend.post@it-university.nl

Question 1415

An IS auditor is reviewing the results of a business process improvement project. Which of the following should be performed FIRST?

- ☒ Evaluate control gaps between the old and the new processes.
- ☐ Develop compensating controls.
- ☐ Document the impact of control weaknesses in the process.
- ☐ Ensure that lessons learned during the change process are documented.

Question 1416

What are used as the framework for developing logical access controls?

- ☒ Information systems security policies
- ☐ Organizational security policies
- ☐ Access Control Lists (ACL)
- ☐ Organizational charts for identifying roles and responsibilities

Explanation:

Explanation:

Information systems security policies are used as the framework for developing logical access controls.

Question 1417

Which of the following should concern an IS auditor when reviewing security in a client- server environment?

- ☐ Protecting data using an encryption technique
- ☐ Preventing unauthorized access using a diskless workstation
- ☒ The ability of users to access and modify the database directly
- ☐ Disabling floppy drives on the users' machines

Explanation:

Explanation:

For the purpose of data security in a client-server environment, an IS auditor should be concerned with the user's ability to access and modify a database directly. This could affect the integrity of the data in the database. Data protected by encryption aid in securing the data. Diskless workstations prevent copying of data into local disks and thus help to maintain the integrity and confidentiality of data. Disabling floppy drives is a physical access control, which helps to maintain the confidentiality of data by preventing it from being copied onto a disk.

Licensed to Berend Post berend.post@it-university.nl

Question 1418

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.

Question 1419

The PRIMARY reason an IS department should analyze past incidents and problems is to:

- ☐ determine if all incidents and problems are reported.
- ☐ assign responsibility for problems.
- ☐ assess help desk performance.
- ☒ identify the causes of recurring incidents and problems.

Question 1420

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Obtaining user approval of program changes is very effective for controlling application changes and maintenance.

Licensed to Berend Post berend.post@it-university.nl

Question 1421

The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- ☐ Utilization of an intrusion detection system to report incidents
- ☐ Mandating the use of passwords to access all software
- ☐ Installing an efficient user log system to track the actions of each user
- ☒ Training provided on a regular basis to all current and new employees

Explanation:

Explanation:

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

Question 1422

Which of the following factors will BEST promote effective information security management?

- ☒ Senior management commitment
- ☐ Identification and risk assessment of sensitive resources
- ☐ Security awareness training
- ☐ Security policy framework

Question 1423

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'.

Licensed to Berend Post berend.post@it-university.nl

Question 1424

ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?

- ☐ Reliability
- ☐ Usability
- ☒ Functionality
- ☐ Maintainability

Explanation:

Explanation:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties.

The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

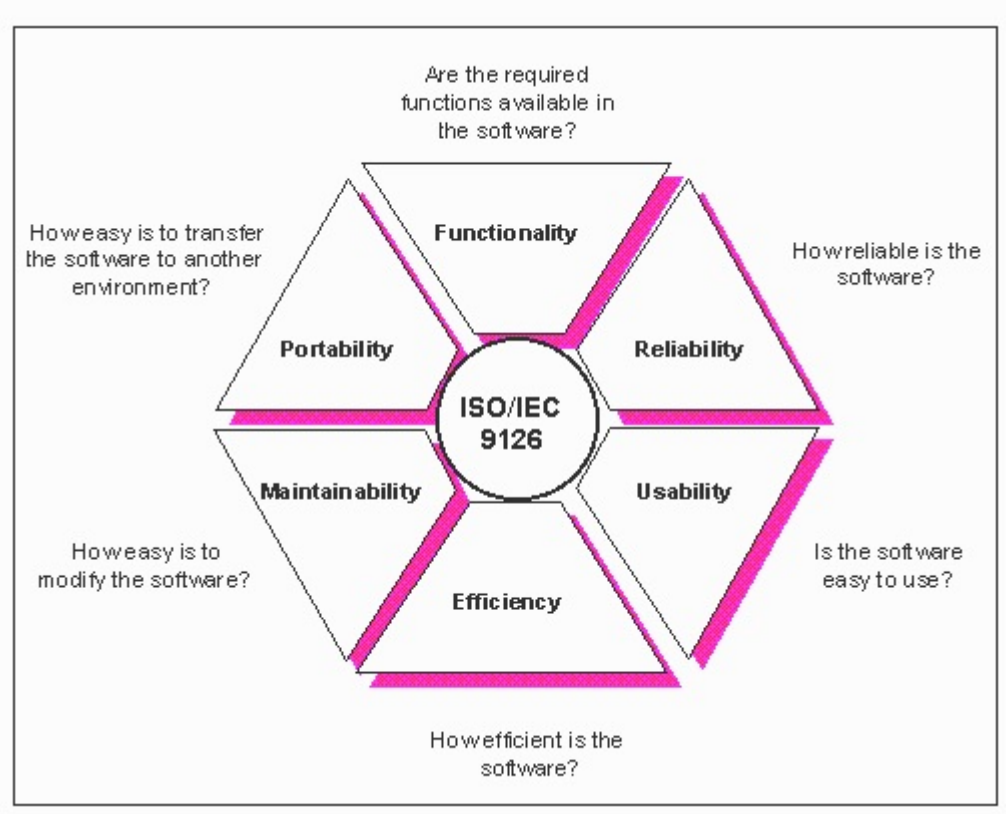
Functionality Compliance

For CISA Exam you should know below information about ISO 9126 model:

ISO/IEC 9126 Software engineering — Product quality was an international standard for the evaluation of software quality. It has been replaced by ISO/IEC 25010:2011.[1] The fundamental objective of the ISO/IEC 9126 standard is to address some of the well-known human biases that can adversely affect the delivery and perception of a software development project. These biases include changing priorities after the start of a project or not having any clear definitions of "success." By clarifying, then agreeing on the project priorities and subsequently converting abstract priorities (compliance) to measurable values (output data can be validated against schema X with zero intervention), ISO/IEC 9126 tries to develop a common understanding of the project's objectives and goals.

ISO 9126

Licensed to Berend Post berend.post@it-university.nl



The standard is divided into four parts:

Quality model

External metrics

Internal metrics

Quality in use metrics.

Quality Model

The quality model presented in the first part of the standard, ISO/IEC 9126-1,[2] classifies software quality in a structured set of characteristics and sub-characteristics as follows:

Functionality - A set of attributes that bear on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs.

Suitability

Accuracy

Interoperability

Security

Functionality Compliance

Licensed to Berend Post berend.post@it-university.nl

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Maturity

Fault Tolerance

Recoverability

Reliability Compliance

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

Understandability

Learn ability

Operability

Attractiveness

Usability Compliance

Efficiency - A set of attributes that bear on the relationship between the level of performance of the software and the amount of resources used, under stated conditions.

Time Behavior

Resource Utilization

Efficiency Compliance

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

Analyzability

Changeability

Stability

Testability

Maintainability Compliance

Portability - A set of attributes that bear on the ability of software to be transferred from one environment to another.

Adaptability

Install ability

Licensed to Berend Post berend.post@it-university.nl

Co-Existence

Replace ability

Portability Compliance

Each quality sub-characteristic (e.g. adaptability) is further divided into attributes. An attribute is an entity which can be verified or measured in the software product. Attributes are not defined in the standard, as they vary between different software products.

Software product is defined in a broad sense: it encompasses executables, source code, architecture descriptions, and so on. As a result, the notion of user extends to operators as well as to programmers, which are users of components such as software libraries.

The standard provides a framework for organizations to define a quality model for a software product. On doing so, however, it leaves up to each organization the task of specifying precisely its own model. This may be done, for example, by specifying target values for quality metrics which evaluates the degree of presence of quality attributes.

Internal Metrics

Internal metrics are those which do not rely on software execution (static measure)

External Metrics

External metrics are applicable to running software.

Quality in Use Metrics

Quality in use metrics are only available when the final product is used in real conditions.

Ideally, the internal quality determines the external quality and external quality determines quality in use.

This standard stems from the GE model for describing software quality, presented in 1977 by McCall et al., which is organized around three types of Quality Characteristics:

Factors (To specify): They describe the external view of the software, as viewed by the users.

Criteria (To build): They describe the internal view of the software, as seen by the developer.

Metrics (To control): They are defined and used to provide a scale and method for measurement.

Licensed to Berend Post berend.post@it-university.nl

ISO/IEC 9126 distinguishes between a defect and a nonconformity, a defect being The nonfulfillment of intended usage requirements, whereas a nonconformity is The nonfulfillment of specified requirements. A similar distinction is made between validation and verification, known as V&V in the testing trade.

The following were incorrect answers:

Reliability - A set of attributes that bear on the capability of software to maintain its level of performance under stated conditions for a stated period of time.

Usability - A set of attributes that bear on the effort needed for use, and on the individual assessment of such use, by a stated or implied set of users.

Maintainability - A set of attributes that bear on the effort needed to make specified modifications.

Reference:

CISA review manual 2014 Page number 188

Question 1425

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 1426

The FIRST step in data classification is to:

- ☒ establish ownership.
- ☐ perform a criticality analysis.
- ☐ define access rules.
- ☐ create a data dictionary.

Explanation:

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

Licensed to Berend Post berend.post@it-university.nl

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 1427

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 1428

An employee uses a personal mobile device to access corporate data and email, but also allows friends to use it as a mobile hotspot for Internet access when not at work. The information security manager is concerned this situation may expose confidential data. The manager's FIRST step should be to:

- ☒ update the mobile device usage standards to address the issue and communicate to all employees
- ☐ activate the incident response plan to mitigate the impact and stop the compromise
- ☐ review the associated risks to determine if additional controls are needed
- ☐ implement additional security controls that will mitigate the situation and then reassess risks

Question 1429

In which phase of penetration testing would host detection and domain name system (DNS) interrogation be performed?

- ☐ Reporting
- ☐ Attacks
- ☒ Discovery
- ☐ Planning

Licensed to Berend Post berend.post@it-university.nl

Question 1430

An IS auditor should carefully review the functional requirements in a system-development project to ensure that the project is designed to:

- ☒ Meet business objectives
- ☐ Enforce data security
- ☐ Be culturally feasible
- ☐ Be financially feasible

Explanation:

Explanation:

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to meet business objectives.

Question 1431

Which of the following is the BEST way to control the concurrent use of licensed software?

- ☐ User self-discipline.
- ☒ Monitor by system administrator.
- ☐ Surprise audit conducted by vendors.
- ☐ Metering software

Question 1432

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 1433

An IS auditor found that a company executive is encouraging employee use of social networking sites for business purposes. Which of the following recommendations would BEST help to reduce the risk of data leakage?

- ☐ Requiring policy acknowledgment and nondisclosure agreements signed by employees
- ☒ Providing education and guidelines to employees on use of social networking sites
- ☐ Establishing strong access controls on confidential data
- ☐ Monitoring employees' social networking usage

Licensed to Berend Post berend.post@it-university.nl

Question 1434

Which of the following controls is MOST effective in detecting spam?

- ☐ Denying transmission control protocol (TCP) connections in the mail server
- ☐ Refusing Internet protocol (IP) connections at the router
- ☐ Registering the recipient with keepers of spam lists
- ☒ Using heuristic filters based on the content of the message

Question 1435

A database is denormalized in order to:

- ☐ prevent loss of data.
- ☒ increase processing efficiency.
- ☐ ensure data integrity.
- ☐ save storage space.

Question 1436

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)

Question 1437

Which of the following would BEST maintain the integrity of a firewall log?

- ☐ Granting access to log information only to administrators
- ☐ Capturing log events in the operating system layer
- ☐ Writing dual logs onto separate storage media
- ☒ Sending log information to a dedicated third-party log server

Explanation:

Explanation:

Establishing a dedicated third-party log server and logging events in it is the best procedure for maintaining the integrity of a firewall log. When access control to the log server is adequately maintained, the risk of unauthorized log modification will be mitigated, therefore improving the integrity of log information. To enforce segregation of duties, administrators should not have access to log files. This primarily contributes to the assurance of confidentiality rather than integrity. There are many ways to capture log information: through the application layer, network layer, operating systems layer, etc.; however, there is no log integrity advantage in capturing events in the operating systems layer. If it is a highly mission-critical information system, it may be nice to run the system

Licensed to Berend Post berend.post@it-university.nl

with a dual log mode. Having logs in two different storage devices will primarily contribute to the assurance of the availability of log information, rather than to maintaining its integrity.

Question 1438

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 1439

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 1440

The use of symmetric key encryption controls to protect sensitive data transmitted over a communications network requires that:

- ☒ primary keys for encrypting the data be stored in encrypted form.
- ☐ encryption keys be changed only when a compromise is detected at both ends.
- ☐ encryption keys at one end be changed on a regular basis.
- ☐ public keys be stored in encrypted form.

Licensed to Berend Post berend.post@it-university.nl

Question 1441

While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

- ☐ recommend the use of disk mirroring.
- ☐ review the adequacy of offsite storage.
- ☒ review the capacity management process.
- ☐ recommend the use of a compression algorithm.

Explanation:

Explanation:

Capacity management is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively. Business criticality must be considered before recommending a disk mirroring solution and offsite storage is unrelated to the problem.

Though data compression may save disk space, it could affect system performance.

Question 1442

Which of the following is the MOST important consideration when developing an online business architecture and recovery strategy?

- ☐ Vendors' network security
- ☐ Immediate problem resolution
- ☐ Vendors' financial stability
- ☒ Single points of failure

Question 1443

An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers-one filled with CO2, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

- ☐ The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
- ☒ Both fire suppression systems present a risk of suffocation when used in a closed room.
- ☐ The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).
- ☐ The documentation binders should be removed from the equipment room to reduce potential risks.

Explanation:

Explanation:

Protecting people's lives should always be of highest priority in fire suppression activities. COz and halon both reduce the oxygen ratio in the atmosphere, which can induce serious personal hazards, in

Licensed to Berend Post berend.post@it-university.nl

many countries installing or refilling halon fire suppression systems is not allowed. Although COz and halon are effective and appropriate for fires involving synthetic combustibles and electrical equipment, they are nearly totally ineffective on solid combustibles (wood and paper). Although not of highest priority, removal of the documentation would probably reduce some of the risks.

Question 1444

Which of the following is the MOST significant risk when an application uses individual end user accounts to access the underlying database?

- ☒ User accounts may remain active after a termination.
- ☐ Multiple connects to the database are used and slow the process.
- ☐ Application may not capture a complete audit trail.
- ☐ Users may be able to circumvent application controls.

Question 1445

Which of the following would help determine the maturity of an information security awareness program?

- ☐ A review of the annual penetration test results
- ☐ A network vulnerability assessment
- ☐ A simulated social engineering test
- ☒ A gap assessment against an established model

Question 1446

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1447

Establishing data ownership is an important first step for which of the following processes?

- ☐ Assigning user access privileges
- ☐ Developing organizational security policies
- ☐ Creating roles and responsibilities
- ☒ Classifying data

Explanation:

Explanation:

To properly implement data classification, establishing data ownership is an important first step.

Question 1448

An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

- ☐ Project sponsor
- ☐ System development project team (SPDT)
- ☒ Project steering committee
- ☐ User project team (UPT)

Explanation:

Explanation:

A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

Licensed to Berend Post berend.post@it-university.nl

Question 1449

An IS auditor performing an audit of backup procedures observes that backup tapes are picked up weekly and stored offsite at a third-party hosting facility. Which of the following recommendations would be the BEST way to maintain data integrity during transport?

- ☒ Ensure the data is transported in locked tamper-evident containers.
- ☐ Ensure that logging and recording of data transport takes place.
- ☐ Ensure the transport company is licensed and insured.
- ☐ Ensure the data is validated prior to transport.

Question 1450

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 1451

What type of approach to the development of organizational policies is often driven by risk assessment?

- ☐ Bottom-up
- ☒ Top-down
- ☐ Comprehensive
- ☐ Integrated

Explanation:

Explanation:

A bottom-up approach to the development of organizational policies is often driven by risk assessment.

Licensed to Berend Post berend.post@it-university.nl

Question 1452

Which of the following is the MOST effective control to ensure electronic records beyond their retention periods are deleted from IT systems?

- ☐ Review the record retention register regularly to initiate data deletion.
- ☒ Build in system logic to trigger data deletion at predefined times.
- ☐ Perform a sample check of current data against the retention schedule.
- ☐ Execute all data deletions at a predefined month during the year.

Question 1453

Which of the following would BEST protect against web-based cross-domain attacks?

- ☐ Network addressing scheme
- ☐ Database hardening
- ☐ Encryption controls
- ☒ Application controls

Question 1454

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 1455

When developing a risk-based IS audit plan, the PRIMARY focus should be on functions:

- ☐ considered important by IT management.
- ☐ with the most ineffective controls.
- ☐ with the greatest number of threats.
- ☒ considered critical to business operations.

Licensed to Berend Post berend.post@it-university.nl

Question 1456

Which of the following would MOST effectively aid executive management in achieving IT and business alignment?

- ☐ Risk assessment
- ☐ Value delivery assessment
- ☒ Balanced scorecard
- ☐ Performance measurement

Question 1457

Which of the following access rights presents the GREATEST risk when granted to a new member of the system development staff?

- ☐ Execute access to development program libraries
- ☐ Write access to development data libraries
- ☐ Execute access to production program libraries
- ☒ Write access to production program libraries

Question 1458

An audit charter should:

- ☐ be dynamic and change often to coincide with the changing nature of technology and the audit profession.
- ☐ clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
- ☐ document the audit procedures designed to achieve the planned audit objectives.
- ☒ outline the overall authority, scope and responsibilities of the audit function.

Explanation:

Explanation:

An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

Licensed to Berend Post berend.post@it-university.nl

Question 1459

Host Based ILD&P primarily addresses the issue of:

- ☐ information integrity
- ☐ information accuracy
- ☐ information validity
- ☒ information leakage
- ☐ None of the choices.

Explanation:

Explanation:

Information Leakage Detection and Prevention (ILD&P) is a computer security term referring to systems designed to detect and prevent the unauthorized transmission of information from the computer systems of an organization to outsiders. Network ILD&P are gateway-based systems installed on the organization's internet network connection and analyze network traffic to search for unauthorized information transmissions. Host Based ILD&P systems run on end-user workstations to monitor and control access to physical devices and access information before it has been encrypted.

Question 1460

The purpose of data migration testing is to validate data:

- ☐ availability.
- ☐ retention.
- ☒ completeness.
- ☐ confidentiality.

Question 1461

Which of the following types of firewalls provide the GREATEST degree and granularity of control?

- ☐ Screaming router
- ☐ Packet filter
- ☒ Application gateway
- ☐ Circuit gateway

Explanation:

Explanation:

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This means that it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and BJ work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4, and not from higher levels. A circuit gateway (choice D) is based on a proxy or program that acts as an intermediary between external and internal

Licensed to Berend Post berend.post@it-university.nl

accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy (which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

Question 1462

Which of the following management decisions presents the GREATEST risk associated with data leakage?

- ☒ Security awareness training is not provided to staff.
- ☐ There is no requirement for desktops to be encrypted.
- ☐ Security policies have not been updated in the past year.
- ☐ Staff are allowed to work remotely.

Question 1463

During a business continuity audit, an IS auditor found that the business continuity plan (BCP) covers 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 the 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 1464

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 1465

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 1466

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:

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

Reference:

CISA Review Manual 2014 Page number 51

and

Official ISC2 guide to CISSP CBK 3rd edition page number 534-539

Question 1467

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).

Question 1468

Which of the following controls would BEST ensure that payroll system rate changes are valid?

- ☐ Only a payroll department manager can input the new rate.
- ☐ Rate changes require visual verification before acceptance.
- ☐ Rate changes must be entered twice to ensure that they are entered correctly.
- ☒ Rate changes are reported to and independently verified by a manager.

Question 1469

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:

Licensed to Berend Post berend.post@it-university.nl

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 1470

Which of the following BEST indicates a need to review an organization's information security policy?

- ☐ Completion of annual IT risk assessment
- ☒ Increasing complexity of business transactions
- ☐ Increasing exceptions approved by management
- ☐ High number of low-risk findings in the audit report

Question 1471

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.

Question 1472

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- ☒ performance measurement.
- ☐ strategic alignment.
- ☐ value delivery.
- ☐ resource management.

Explanation:

Explanation:

Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver {process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans.

Licensed to Berend Post berend.post@it-university.nl

Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

Question 1473

A benefit of open system architecture is that it:

- ☒ facilitates interoperability.
- ☐ facilitates the integration of proprietary components.
- ☐ will be a basis for volume discounts from equipment vendors.
- ☐ allows for the achievement of more economies of scale for equipment.

Explanation:

Explanation:

Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

Question 1474

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1475

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 1476

Which of the following provides the MOST reliable audit evidence on the validity of transactions in a financial application?

- ☒ Substantive testing
- ☐ Walk-through reviews
- ☐ Compliance testing
- ☐ Design documentation reviews

Question 1477

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1478

Which of the following governance functions is responsible for ensuring IT projects have sufficient resources and are prioritized appropriately?

- ☐ Board of directors
- ☐ IT management
- ☒ IT steering committee
- ☐ Executive management

Question 1479

An IS auditor notes that a loan servicing group retains customer personally identifiable information (PII) on a shared drive. Which of the following is MOST important to ensure compliance with privacy principles?

- ☐ Backups are performed in accordance with organizational policy.
- ☐ Access to the shared drive must be approved by the manager of the group.
- ☒ The data is maintained in accordance with the business's retention policy.
- ☐ All key customer data elements are captured on the shared drive.

Question 1480

Which of the following methods would be MOST effective in verifying that all changes have been authorized?

- ☐ Reconciling problem tickets with authorized change control entries
- ☐ Reconciling reports of changes in production libraries to authorized change log entries
- ☒ Validating authorized change log entries with individual(s) who promoted into production
- ☐ Reconciling reports of changes in development libraries to supporting documentation

Question 1481

An organization implements a data loss prevention tool as a control to mitigate the risk of sensitive data leaving the organization via electronic mail. Which of the following would provide the BEST indication of adequate control design?

- ☐ Management has formally approved the control design.
- ☐ Management presents evidence that data loss incidents have decreased.
- ☒ Security administrators can demonstrate the functions of the tool.
- ☐ Rules enforced by the tool were based on the classification of the data.

Licensed to Berend Post berend.post@it-university.nl

Question 1482

Hamid needs to shift users from using the application from the existing (Old) system to the replacing (new) system. His manager Lily has suggested he uses an approach in which the newer system is changed over from the older system on a cutoff date and time and the older system is discontinued once the changeover to the new system takes place. Which of the following changeover approach is suggested by Lily?

- ☐ Parallel changeover
- ☐ Phased changeover
- ☒ Abrupt changeover
- ☐ Pilot changeover

Explanation:

Explanation:

In the abrupt changeover approach the newer system is changed over from the older system on a cutoff date and time, and the older system is discontinued once changeover to the new system takes place.

Changeover refers to an approach to shift users from using the application from the existing (old) system to the replacing (new) system.

Changeover to newer system involves four major steps or activities

Conversion of files and programs; test running on test bed

Installation of new hardware, operating system, application system and the migrated data.

Training employees or user in groups

Scheduling operations and test running for go-live or changeover

Some of the risk areas related to changeover includes:

Asset safeguarding

Data integrity

System effectiveness

Change management challenges

Duplicate or missing records

The following were incorrect answers:

Licensed to Berend Post berend.post@it-university.nl

Parallel changeover – This technique includes running the old system, then running both the old and new systems in parallel and finally full changing over to the new system after gaining confidence in the working of new system.

Phased Changeover -In this approach the older system is broken into deliverables modules. Initially, the first module of older system is phased out using the first module of a new system. Then, the second module of the newer system is phased out, using the second module of the newer system and so forth until reaching the last module.

Pilot changeover – Not a valid changeover type.

Reference:

CISA review manual 2014 Page number 172

Question 1483

Which of the following documents would be MOST useful in detecting a weakness in segregation of duties?

- ☐ Entity-relationship diagram
- ☒ Process flowchart
- ☐ Data flow diagram
- ☐ Systems flowchart

Question 1484

An information security manager has discovered a potential security breach in a server that supports a critical business process. Which of the following should be the information security manager's FIRST course of action?

- ☒ Validate that there has been an incident
- ☐ Notify the business process owner
- ☐ Shut down the server in an organized manner
- ☐ Inform senior management of the incident

Licensed to Berend Post berend.post@it-university.nl

Question 1485

Which of the following sampling methods is the BEST approach for drawing conclusions based on frequency of occurrence?

- ☐ Attribute sampling
- ☒ Monetary estimation sampling
- ☐ Stratified sampling
- ☐ Difference estimation sampling

Question 1486

At what point in software development should the user acceptance test plan be prepared?

- ☐ Implementation planning
- ☐ Requirements definition
- ☐ Transfer into production
- ☒ Feasibility study

Question 1487

An IS auditor identifies key controls that have been overridden by management. The NEXT step the IS auditor should take is to:

- ☐ perform procedures to quantify the irregularities.
- ☒ report the absence of key controls to regulators.
- ☐ recommend compensating controls.
- ☐ withdraw from the engagement.

Question 1488

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1489

What is an IS auditor's BEST recommendation to management if a review of the incident management process finds multiple instances of incident tickets remaining open for an unusually long time?

- ☐ Implement reporting of key performance indicators (KPIs) for ticket closure.
- ☐ Increase the number of help desk staff to enable faster ticket closure.
- ☐ Manually review the identified tickets and mark as closed in the system.
- ☒ Configure the system to automatically close tickets after a defined period.

Question 1490

Why is it not preferable for a firewall to treat each network frame or packet in isolation?

- ☒ Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- ☐ Such a firewall is costly to setup.
- ☐ Such a firewall is too complicated to maintain.
- ☐ Such a firewall is CPU hungry.
- ☐ Such a firewall offers poor compatibility.
- ☐ None of the choices.

Explanation:

Explanation:

A stateless firewall treats each network frame or packet in isolation.

Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

Question 1491

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

Licensed to Berend Post berend.post@it-university.nl

Question 1492

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- ☐ digest signature.
- ☐ electronic signature.
- ☒ digital signature.
- ☐ hash signature.

Explanation:

Explanation:

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

Question 1493

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- ☒ topology diagrams.
- ☐ bandwidth usage.
- ☐ traffic analysis reports.
- ☐ bottleneck locations.

Explanation:

Explanation:

The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

Question 1494

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

Licensed to Berend Post berend.post@it-university.nl

risk of an unauthorized person following an authorized person through a secured entry (piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

Question 1495

The logical exposure associated with the use of a checkpoint restart procedure is:

- ☐ denial of service.
- ☒ an asynchronous attack
- ☐ wire tapping.
- ☐ computer shutdown.

Explanation:

Explanation:

Asynchronous attacks are operating system-based attacks. A checkpoint restart is a feature that stops a program at specified intermediate points for later restart in an orderly manner without losing data at the checkpoint. The operating system saves a copy of the computer programs and data in their current state as well as several system parameters describing the mode and security level of the program at the time of stoppage. An asynchronous attack occurs when an individual with access to this information is able to gain access to the checkpoint restart copy of the system parameters and change those parameters such that upon restart the program would function at a higher-priority security level.

Question 1496

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 1497

Why does an IS auditor review an organization chart?

- ☐ To optimize the responsibilities and authority of individuals
- ☐ To control the responsibilities and authority of individuals
- ☒ To better understand the responsibilities and authority of individuals
- ☐ To identify project sponsors

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

Question 1498

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 1499

An IS auditor previously worked in an organization's IT department and was involved with the design of the business continuity plan (BCP). The IS auditor has now been asked to review this same BCP. The auditor should FIRST:

- ☐ document the conflict in the audit report.
- ☐ decline the audit assignment.
- ☐ communicate the conflict of interest to the audit manager prior to starting the assignment.
- ☒ communicate the conflict of interest to the audit committee prior to starting the assignment.

Question 1500

When an operating system is being hardened, it is MOST important for an information security manager to ensure that:

- ☒ default passwords are changed.
- ☐ anonymous access is removed.
- ☐ file access is restricted.
- ☐ system logs are activated.

Question 1501

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:

Licensed to Berend Post berend.post@it-university.nl

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 1502

Structured programming is BEST described as a technique that:

- ☐ provides knowledge of program functions to other programmers via peer reviews.
- ☒ reduces the maintenance time of programs by the use of small-scale program modules.
- ☐ makes the readable coding reflect as closely as possible the dynamic execution of the program.
- ☐ controls the coding and testing of the high-level functions of the program in the development process.

Explanation:

Explanation:

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well-known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

Question 1503

Which of the following would be MOST helpful when assessing how applications exchange data with other applications?

- ☐ List of servers and their applications
- ☒ Entity relationship diagram
- ☐ Results of a risk assessment on the applications
- ☐ Configuration management database

Licensed to Berend Post berend.post@it-university.nl

Question 1504

Which of the following antispam filtering techniques would BEST prevent a valid, variable- length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

- ☐ Heuristic (rule-based)
- ☐ Signature-based
- ☐ Pattern matching
- ☒ Bayesian (statistical)

Explanation:

Explanation:

Bayesian filtering applies statistical modeling to messages, by performing a frequency analysis on each word within the message and then evaluating the message as a whole. Therefore, it can ignore a suspicious keyword if the entire message is within normal bounds. Heuristic filtering is less effective, since new exception rules may need to be defined when a valid message is labeled as spam. Signature-based filtering is useless against variable- length messages, because the calculated MD5 hash changes all the time. Finally, pattern matching is actually a degraded rule- based technique, where the rules operate at the word level using wildcards, and not at higher levels.

Question 1505

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 1506

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:

Explanation:

Confidentiality supports the principle of "least privilege" by providing that only authorized individuals, processes, or systems should have access to information on a need-to-know basis.

Licensed to Berend Post berend.post@it-university.nl

The level of access that an authorized individual should have is at the level necessary for them to do their job. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information.

Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources.

An important measure to ensure confidentiality of information is data classification. This helps to determine who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practices that support maintaining the confidentiality of information.

A sample control for protecting confidentiality is to encrypt information. Encryption of information limits the usability of the information in the event it is accessible to an unauthorized person.

For your exam you should know the information below:

Integrity

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Information stored in files, databases, systems, and networks must be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices.

Sample controls include management controls such as segregation of duties, approval checkpoints in the systems development life cycle, and implementation of testing practices that assist in providing information integrity. Well-formed transactions and security of the update programs provide consistent methods of applying changes to systems. Limiting update access to those individuals with a need to access limits the exposure to intentional and unintentional modification.

Availability

Availability is the principle that ensures that information is available and accessible to users when needed.

The two primary areas affecting the availability of systems are:

Licensed to Berend Post berend.post@it-university.nl

1. Denial-of-Service attacks and

2. Loss of service due to a disaster, which could be man-made (e.g., poor capacity planning resulting in system crash, outdated hardware, and poor testing resulting in system crash after upgrade) or natural (e.g., earthquake, tornado, blackout, hurricane, fire, and flood).

In either case, the end user does not have access to information needed to conduct business. The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes. The lack of appropriate security controls can increase the risk of viruses, destruction of data, external penetrations, or denial-of-service (DOS) attacks. Such events can prevent the system from being used by normal users.

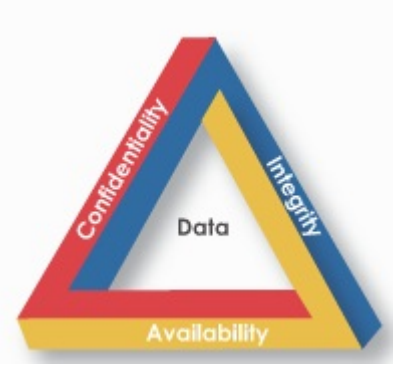
CIA

The following answers are incorrect:

Integrity- Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes.

Availability - Availability is the principle that ensures that information is available and accessible to users when needed.

Accuracy – Accuracy is not a valid CIA attribute.



Reference:

CISA review manual 2014 Page number 314

Official ISC2 guide to CISSP CBK 3rd Edition Page number 350

Licensed to Berend Post berend.post@it-university.nl

Question 1507

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 1508

Which of the following control is intended to discourage a potential attacker?

- ☒ Deterrent
- ☐ Preventive
- ☐ Corrective
- ☐ Recovery

Explanation:

Explanation:

Deterrent Control are intended to discourage a potential attacker

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

Licensed to Berend Post berend.post@it-university.nl

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events.

When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs.

It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will determine most employees from installing wireless access points.

Preventative Controls

Preventive controls are intended to avoid an incident from occurring. Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control

rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

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.

Licensed to Berend Post berend.post@it-university.nl

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

Licensed to Berend Post berend.post@it-university.nl

deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

Preventive - Preventive controls are intended to avoid an incident from occurring

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

Reference:

CISA Review Manual 2014 Page number 44

and

Official ISC2 CISSP guide 3rd edition Page number 50 and 51

Question 1509

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1510

A company uses a standard form to document and approve all changes in production programs. To ensure that the forms are properly authorized, which of the following is the MOST effective sampling method?

- ☒ Attribute
- ☐ Variable
- ☐ Discovery
- ☐ Monetary

Question 1511

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 1512

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:

Licensed to Berend Post berend.post@it-university.nl

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 1513

A maturity model is useful in the assessment of IT service management because it:

- ☒ provides a benchmark for process improvement
- ☐ defines the level of control required to meet business needs
- ☐ indicates the service levels required for the business area
- ☐ specifies the mechanism needed to achieve defined service levels

Question 1514

When auditing a proxy-based firewall, an IS auditor should:

- ☐ verify that the firewall is not dropping any forwarded packets.
- ☐ review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
- ☒ verify that the filters applied to services such as HTTP are effective.
- ☐ test whether routing information is forwarded by the firewall.

Explanation:

Explanation:

A proxy-based firewall works as an intermediary (proxy) between the service or application and the client, it makes a connection with the client and opens a different connection with the server and, based on specific filters and rules, analyzes all the traffic between the two connections.

Unlike a packet-filtering gateway, a proxy-based firewall does not forward any packets. Mapping between media access control (MAC) and IP addresses is a task for protocols such as Address Resolution Protocol/Reverse Address Resolution Protocol (ARP/RARP).

Question 1515

Which of the following findings would be of GREATEST concern to an IS auditor performing an information security audit of critical server log management activities?

- ☒ Log records can be overwritten before being reviewed.
- ☐ Logging procedures are insufficiently documented.
- ☐ Log records are dynamically into different servers.
- ☐ Logs are monitored using manual processes.

Licensed to Berend Post berend.post@it-university.nl

Question 1516

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- ☐ control self-assessments.
- ☐ a business impact analysis.
- ☒ an IT balanced scorecard.
- ☐ business process reengineering.

Explanation:

Explanation:

An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. Control self- assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

Question 1517

A bank is selecting a server for its retail accounts application. To ensure that the server can handle a high volume of transactions with the required response times, which test should the IS auditor recommend?

- ☐ Regression
- ☐ Acceptance
- ☒ Benchmark
- ☐ Integration

Question 1518

An enterprise receiving email should have procedures to control:

- ☐ insufficient end-points.
- ☒ unsolicited executable code.
- ☐ outdated protocols.
- ☐ insufficient connectivity.

Question 1519

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 1520

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.

Question 1521

An organization is in the process of deciding whether to allow a bring your own device (BYOD) program. If approved, which of the following should be the FIRST control required before implementation?

- ☐ Device baseline configurations
- ☒ Device registration
- ☐ An acceptable use policy
- ☐ An awareness program

Question 1522

What should be the GREATEST concern to an IS auditor when employees use portable media (MP3 players, flash drives)?

- ☒ The copying of sensitive data on them
- ☐ The copying of songs and videos on them
- ☐ The cost of these devices multiplied by all the employees could be high
- ☐ They facilitate the spread of malicious code through the corporate network

Explanation:

Explanation:

The MAIN concern with MP3 players and flash drives is data leakage, especially sensitive information. This could occur if the devices were lost or stolen. The risk when copying songs and videos is copyright infringement, but this is normally a less important risk than information leakage. Choice C is hardly an issue because employees normally buy the portable media with their own funds. Choice

Licensed to Berend Post berend.post@it-university.nl

D is a possible risk, but not as important as information leakage and can be reduced by other controls.

Question 1523

Which of the following is the PRIMARY purpose of conducting a business impact analysis (BIA)?

- ☐ Identifying risk mitigation options
- ☒ Identifying key business risks
- ☐ Identifying critical business processes
- ☐ Identifying the threat environment

Question 1524

Which of the following findings would be of GREATEST concern to an IS auditor reviewing an organization's newly implemented online security awareness program?

- ☐ Only new employees are required to attend the program
- ☐ The timing for program updates has not been determined
- ☒ Metrics have not been established to assess training results
- ☐ Employees do not receive immediate notification of results

Question 1525

An organization has decided to migrate payroll processing to a new platform hosted by a third party in a different country. Which of the following is MOST important for the IS auditor to consider?

- ☐ The service provider's compliance with privacy regulations
- ☐ Whether the contract contains a right-to-terminate clause
- ☒ The service provider's compliance with financial regulations
- ☐ Storage costs charged by the service provider

Question 1526

IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through

Licensed to Berend Post berend.post@it-university.nl

compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

Question 1527

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- ☐ Discussion with management
- ☐ Review of the organization chart
- ☒ Observation and interviews
- ☐ Testing of user access rights

Explanation:

Explanation:

By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

Question 1528

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 1529

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 1530

Overall responsibility for approving logical access rights to information assets should reside with the:

- ☒ data and systems owners.
- ☐ systems delivery and operations group.
- ☐ security administrator.
- ☐ systems administrator.

Question 1531

Which of the following transmission media is LEAST vulnerable to cross talk?

- ☐ Copper cable
- ☒ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Explanation:

Explanation:

Fiber optics cables are used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

For your exam you should know below information about transmission media:

Copper Cable

Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.

Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Licensed to Berend Post berend.post@it-university.nl

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable is expensive and does not support many LAN's. It supports data and video.

Coaxial Cable

Licensed to Berend Post berend.post@it-university.nl

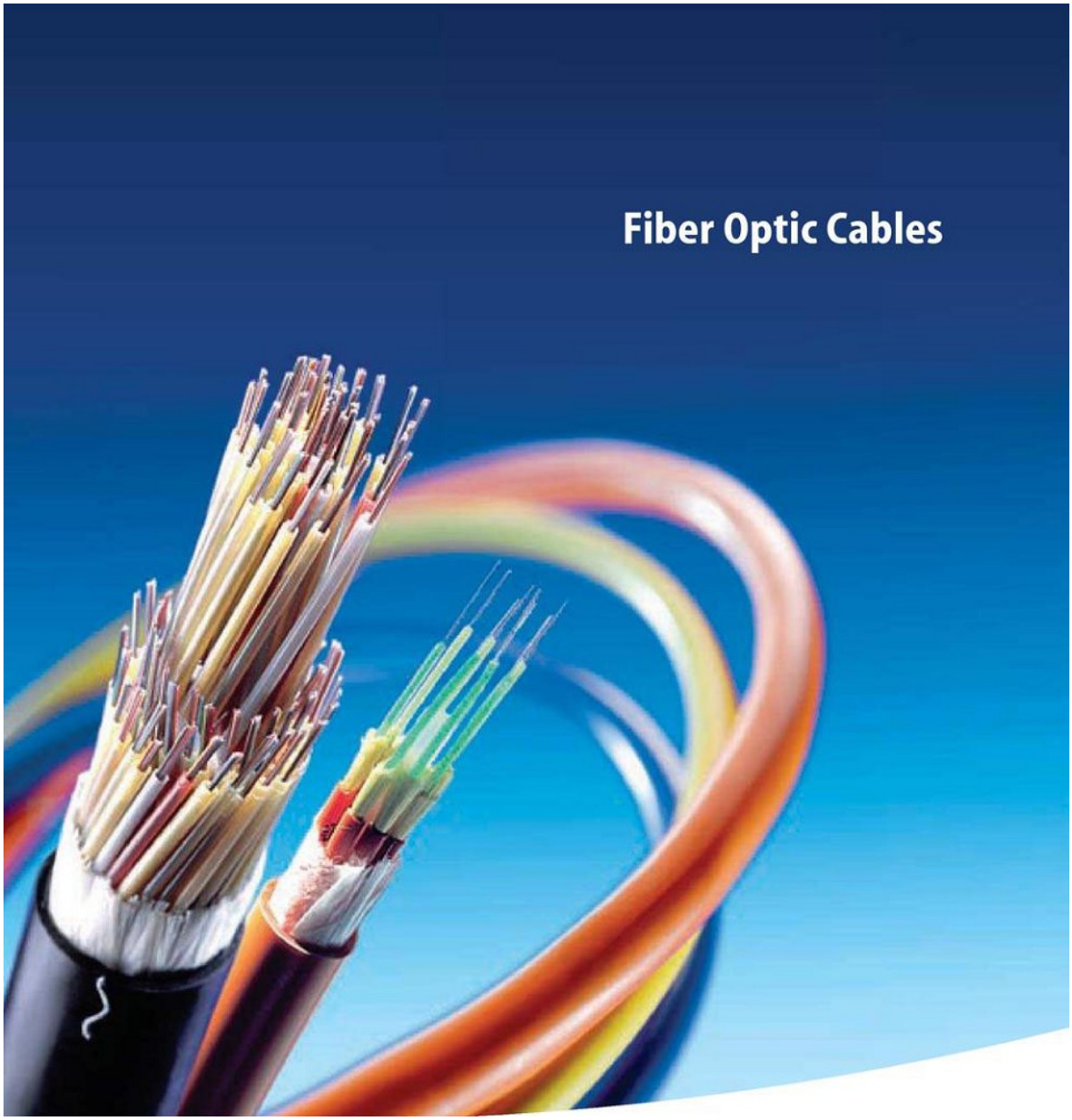
Fiber optics

An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.

Fiber Optics

Licensed to Berend Post berend.post@it-university.nl



Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimeter; these are called microwaves.

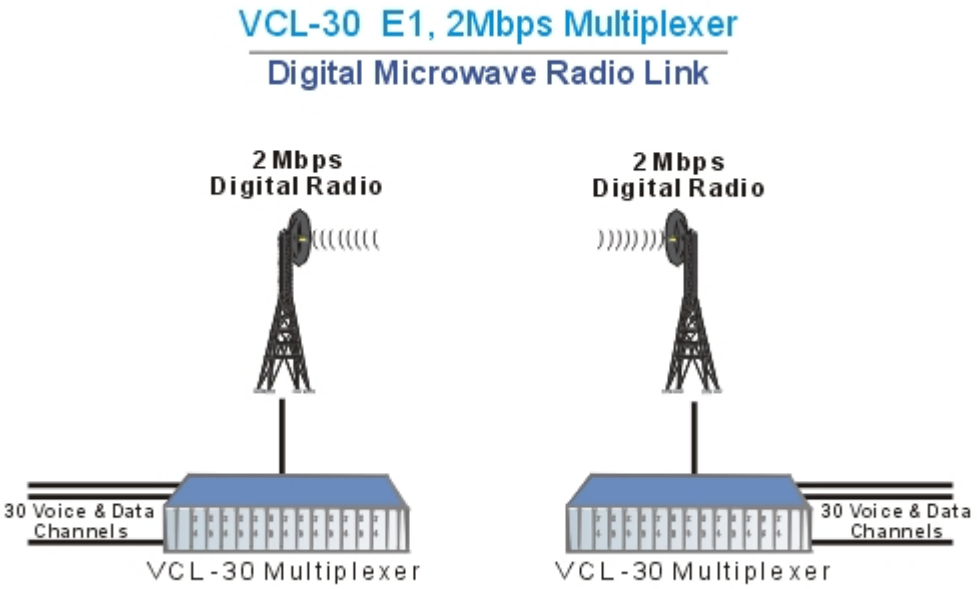
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Licensed to Berend Post berend.post@it-university.nl

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to intercept.

Microwave Radio System



Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to intercept.

Radio System

Radio systems are used for short distance, cheap and easy to tap.

Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Licensed to Berend Post berend.post@it-university.nl

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

The following answers are incorrect:

Copper Cable- Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

Coaxial cable - Coaxial cable are expensive and does not support many LAN's. It supports data and video

Reference:

CISA review manual 2014 page number 265

Question 1532

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:

Explanation:

Key management is better in asymmetric key encryption as compare to symmetric key encryption. In fact, there is no key management built within Symmetric Crypto systems. You must use the sneaker net or a trusted courier to exchange the key securely with the person you wish to communicate with.

Key management is the major issue and challenge in symmetric key encryption.

In symmetric key encryption, a symmetric key is shared between two users who wish to communicate together. As the number of users grows, the number of keys required also increases very rapidly.

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

CISA review manual 2014 Page number 348

Question 1533

Which of the following BEST addresses the availability of an online store?

- ☐ Online backups
- ☒ A mirrored site at another location
- ☐ RAID level 5 storage devices
- ☐ Clustered architecture

Licensed to Berend Post berend.post@it-university.nl

Question 1534

Which of the following is a substantive test?

- ☐ Checking a list of exception reports
- ☐ Ensuring approval for parameter changes
- ☒ Using a statistical sample to inventory the tape library
- ☐ Reviewing password history reports

Explanation:

Explanation:

A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

Question 1535

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:

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

Licensed to Berend Post berend.post@it-university.nl

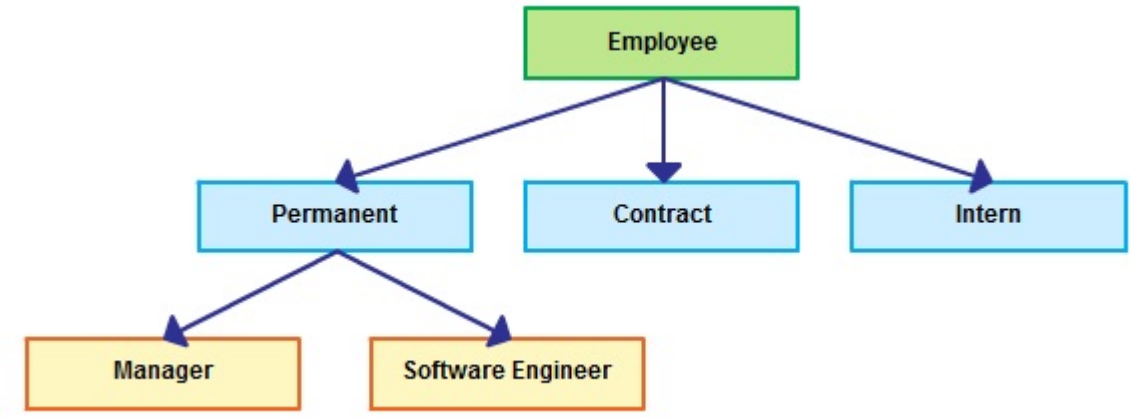
Object-relational database models

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



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

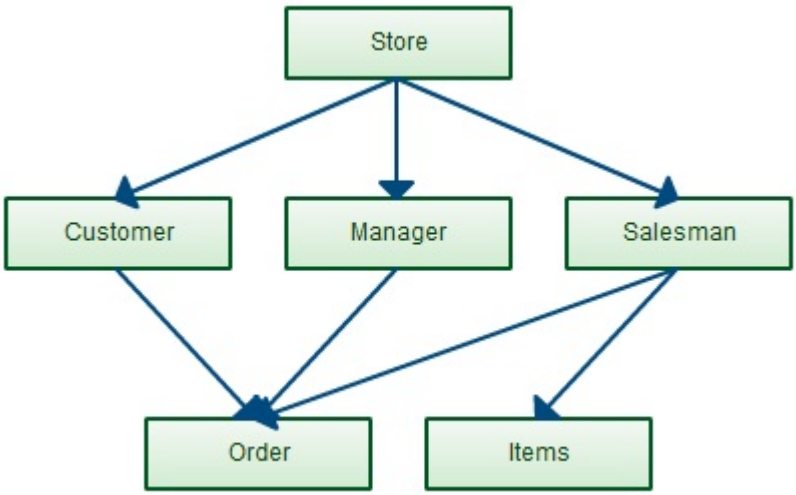
Licensed to Berend Post berend.post@it-university.nl

(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



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".

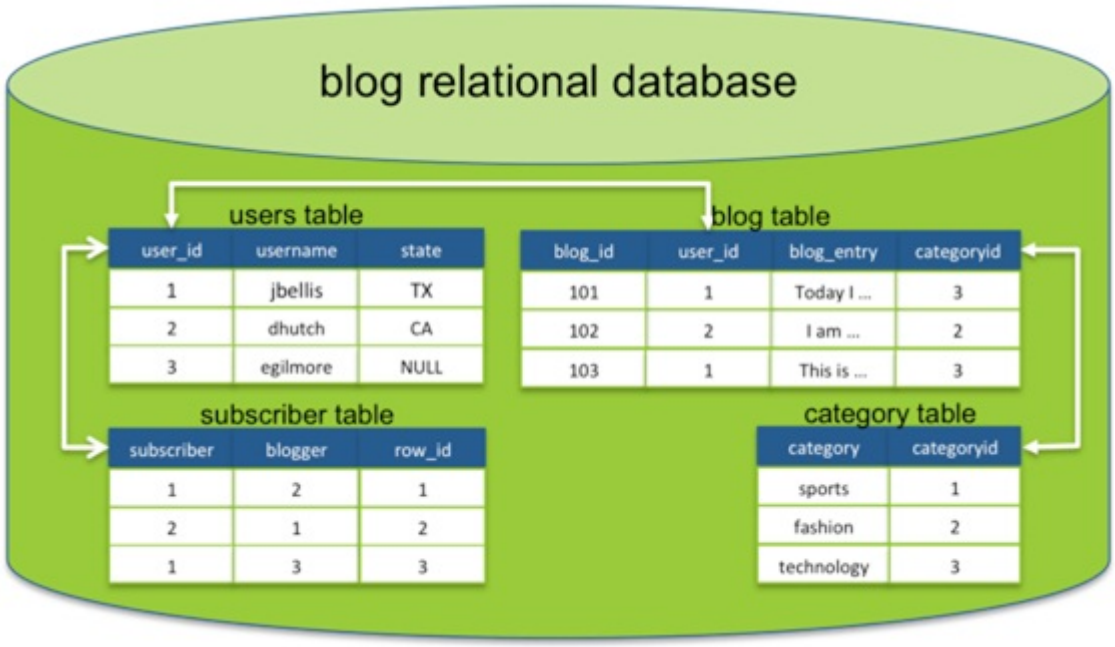
The purpose of the relational model is to provide a declarative method for specifying data and queries: users directly state what information the database contains and what information they want

Licensed to Berend Post berend.post@it-university.nl

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



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.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

Hierarchical database model - In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

Network database model-The network model expands upon the hierarchical structure, allowing many-to-many relationships in a tree-like structure that allows multiple parents.

Object-relational database models- An object-relational database can be said to provide a middle ground between relational databases and object-oriented databases (OODBMS). In object-relational databases, the approach is essentially that of relational databases: the data resides in the database and is manipulated collectively with queries in a query language; at the other extreme are OODBMSes in which the database is essentially a persistent object store for software written in an object-oriented programming language, with a programming API for storing and retrieving objects, and little or no specific support for querying.

Reference:

CISA review manual 2014 Page number 254

Question 1536

Following a security breach in which a hacker exploited a well-known vulnerability in the domain controller, an IS auditor has been asked to conduct a control assessment. The auditor's BEST course of action would be to determine if:

- ☐ the domain controller was classified for high availability.
- ☐ the network traffic was being monitored.
- ☐ the patches were updated.
- ☒ the logs were monitored.

Question 1537

_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

- ☒ Quantitative; qualitative
- ☐ Qualitative; quantitative
- ☐ Residual; subjective
- ☐ Quantitative; subjective

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

Question 1538

As an auditor it is very important to ensure confidentiality, integrity, authenticity and availability are implemented appropriately in an information system. Which of the following definitions incorrectly describes these parameters?

1. Authenticity – A third party must be able to verify that the content of a message has been sent by a specific entity and nobody else.

2. Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

3. Accountability – The action of an entity must be uniquely traceable to different entities
4. Availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

- ☐ All of the options presented
- ☐ None of the options presented
- ☐ Options number 1 and 2
- ☒ Option number 3

Explanation:

Explanation:

It is important to read carefully the question. The word "incorrectly" was the key word. You had to find which one of the definitions presented is incorrect. The definition of Accountability was NOT properly described. Below you have the proper definition.

The correct definitions are as follows

Authenticity – A third party must be able to verify that the content of a message is from a specific entity and nobody else.

Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party. A person cannot deny having sent a message if the message is signed by the originator.

Accountability – The action of an entity must be uniquely traceable to that entity

Licensed to Berend Post berend.post@it-university.nl

Network availability – The IT resource must be available on a timely basis to meet mission requirements or to avoid substantial losses.

Reference:

CISA review manual 2014 Page number 34

Question 1539

Which of the following is the PRIMARY risk when business units procure IT assets without IT involvement?

- ☒ Corporate procurement standards are not followed.
- ☐ The business units want IT to be responsible for maintenance costs.
- ☐ Data security requirements are not considered.
- ☐ System inventory becomes inaccurate.

Question 1540

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 1541

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:

Explanation:

Data Interface enables the expert system to collect data from nonhuman sources, such as measurement instruments in a power plant.

Licensed to Berend Post berend.post@it-university.nl

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.

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

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

CISA review manual 2014 Page number 187

Question 1542

An IS auditor finds an organization has a significant number of systems developed by end-users. Which of the following is the BEST recommendation to help mitigate the associated risks?

- ☐ Storing systems on a shared drive managed by IT
- ☐ Storing developed source code in a centralized repository
- ☐ Centralizing information technology procurement
- ☒ Using a formal development methodology

Licensed to Berend Post berend.post@it-university.nl

Question 1543

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- ☒ an assessment of the fit of the organization's application portfolio with business objectives.
- ☐ actions to reduce hardware procurement cost.
- ☐ a listing of approved suppliers of IT contract resources.
- ☐ a description of the technical architecture for the organization's network perimeter security.

Explanation:

Explanation:

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail ofa specific technical architecture.

Question 1544

An effective implementation of security roles and responsibilities is BEST evidenced across an enterprise when:

- ☒ operational activities are aligned with policies.
- ☐ policies are signed off by users.
- ☐ policies are rolled out and disseminated.
- ☐ reviews and updates of policies are regularly performed.

Question 1545

Intrusion detection systems (IDSs) can:

- ☐ substitute for a firewall.
- ☐ compensate for weak authentication mechanisms.
- ☐ conduct investigations of attacks from within the network.
- ☒ provide information to enhance the security infrastructure.

Licensed to Berend Post berend.post@it-university.nl

Question 1546

Which of the following is an example of audit risk?

- ☐ Audit work may be lost due to a malware attack.
- ☐ Management may disagree with audit conclusions.
- ☒ Sampling methods may not detect a material error.
- ☐ Newer auditors may require additional supervision and training.

Question 1547

Which of the following attack is also known as Time of Check(TOC)/Time of Use(TOU)?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☒ Race Condition

Explanation:

Explanation:

A Race Condition attack is also known as Time of Check(TOC)/Time of Use(TOU).

A race condition is when processes carry out their tasks on a shared resource in an incorrect order. A race condition is possible when two or more processes use a shared resource, as in data within a variable. It is important that the processes carry out their functionality in the correct sequence. If process 2 carried out its task on the data before process 1, the result will be much different than if process1 carried out its tasks on the data before process 2.

In software, when the authentication and authorization steps are split into two functions, there is a possibility an attacker could use a race condition to force the authorization step to be completed before the authentication step. This would be a flaw in the software that the attacker has figured out how to exploit. A race condition occurs when two or more processes use the same resource and the sequences of steps within the software can be carried out in an improper order, something that can drastically affect the output. So, an attacker can force the authorization step to take place before the authentication step and gain unauthorized access to a resource.

The following answers are incorrect:

Eavesdropping - is the act of secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything good of themselves...eavesdroppers always try to listen to matters that concern them."

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.

Reference:

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 1548

A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

- ☐ Unit testing
- ☒ Integration testing
- ☐ Design walk-throughs
- ☐ Configuration management

Explanation:

Explanation:

A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight), units are tested by the programmer, and then transferred to the acceptance test area. This often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

Licensed to Berend Post berend.post@it-university.nl

Question 1549

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 1550

Which of the following is the BEST method for determining the criticality of each application system in the production environment?

- ☐ interview the application programmers.
- ☐ Perform a gap analysis.
- ☐ Review the most recent application audits.
- ☒ Perform a business impact analysis.

Explanation:

Explanation:

A business impact analysis will give the impact of the loss of each application. Interviews with the application programmers will provide limited information related to the criticality of the systems. A gap analysis is only relevant to systems development and project management. The audits may not contain the required information or may not have been done recently.

Question 1551

Who is responsible for restricting and monitoring access of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☒ Security Administrator

Explanation:

Explanation:

Security administrator are responsible for providing adequate and logical security for IS programs, data and equipment.

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

CISA review manual 2014 Page number 361

Licensed to Berend Post berend.post@it-university.nl

Question 1552

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 1553

An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

- ☐ defining the conceptual schema.
- ☐ defining security and integrity checks.
- ☐ liaising with users in developing data model.
- ☒ mapping data model with the internal schema.

Explanation:

Explanation:

A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprise wide view of data within an organization and is the basis for deriving and end-user department data model.

Licensed to Berend Post berend.post@it-university.nl

Question 1554

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- ☒ compromises the Wireless Application Protocol (WAP) gateway.
- ☐ installs a sniffing program in front of the server.
- ☐ steals a customer's PDA.
- ☐ listens to the wireless transmission.

Explanation:

Explanation:

In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised, all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

Question 1555

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 1556

An IS auditor finds ad hoc vulnerability scanning is in place with no clear alignment to the organization's wider security threat and vulnerability management program. Which of the following would BEST enable the organization to work toward improvement in this area?

- ☐ Outsourcing the threat and vulnerability management function to a third party
- ☐ Implementing security logging to enhance threat and vulnerability management
- ☐ Using a capability maturity model to identify a path to an optimized program
- ☒ Maintaining a catalog of vulnerabilities that may impact mission-critical systems

Licensed to Berend Post berend.post@it-university.nl

Question 1557

The PRIMARY role of a control self-assessment (CSA) facilitator is to:

- ☒ report on the internal control weaknesses.
- ☐ focus the team on internal controls.
- ☐ provide solutions for control weaknesses.
- ☐ conduct interviews to gain background information.

Question 1558

Which of the following metrics would BEST measure the agility of an organization's IT function?

- ☒ Average time to turn strategic IT objectives into an agreed upon and approved initiative
- ☐ Average number of learning and training hours per IT staff member
- ☐ Frequency of security assessments against the most recent standards and guidelines
- ☐ Percentage of staff with sufficient IT-related skills for the competency required of their roles.

Question 1559

While reviewing the business continuity plan of an organization, an IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?

- ☐ Deterrence
- ☒ Mitigation
- ☐ Recovery
- ☐ Response

Explanation:

Explanation:

An effective business continuity plan includes steps to mitigate the effects of a disaster. Files must be restored on a timely basis for a backup plan to be effective. An example of deterrence is when a plan includes installation of firewalls for information systems. An example of recovery is when a plan includes an organization's hot site to restore normal business operations.

Question 1560

The PRIMARY responsibility of a project steering committee is to:

- ☐ ensure that each project deadline is met
- ☐ undertake final acceptance of the system for implementation
- ☐ ensure that systems developed meet business needs
- ☒ provide day-to-day guidance and oversight

Licensed to Berend Post berend.post@it-university.nl

Question 1561

How often should a Business Continuity Plan be reviewed?

- ☐ At least once a month
- ☐ At least every six months
- ☒ At least once a year
- ☐ At least Quarterly

Explanation:

Explanation:

As stated in SP 800-34 Rev. 1:

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. During the Operation/Maintenance phase of the SDLC, information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency (at least once a year for the purpose of the exam) or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews.

Remember, there could be two good answers as specified above. Either once a year or whenever significant changes occur to the plan. You will of course get only one of the two presented within your exam.

Reference:

NIST SP 800-34 Revision 1

Question 1562

Which of the following MOST effectively provides assurance of ongoing service delivery by a vendor?

- ☐ Regular status reporting provided by the vendor
- ☐ Short incident response time by the vendor
- ☒ Pre-defined service and operational level agreements
- ☐ Regular monitoring by service management team

Licensed to Berend Post berend.post@it-university.nl

Question 1563

Which of the following is MOST important to consider when developing a disaster recovery plan?

- ☐ Business continuity plan (BCP)
- ☐ Feasibility assessment
- ☒ Business impact analysis (BIA)
- ☐ Cost-benefit analysis

Question 1564

Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

- ☒ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Explanation:

Explanation:

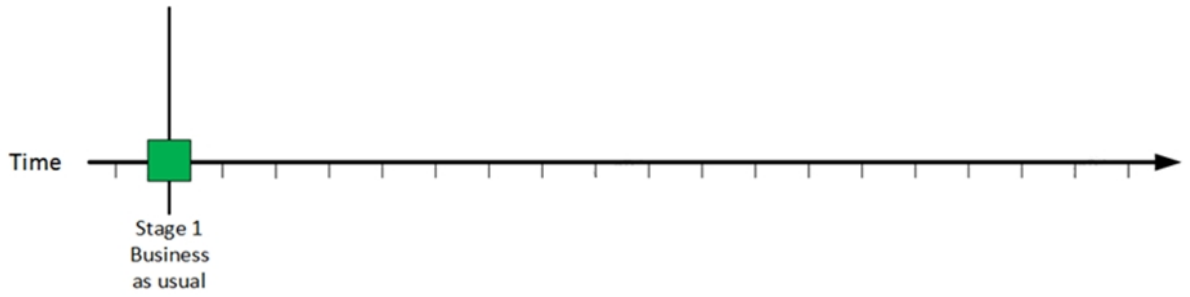
A recovery point objective, or "RPO", is defined by business continuity planning. It is the maximum tolerable period in which data might be lost from an IT service due to a major incident. The RPO gives systems designers a limit to work to. For instance, if the RPO is set to four hours, then in practice, off-site mirrored backups must be continuously maintained – a daily off-site backup on tape will not suffice. Care must be taken to avoid two common mistakes around the use and definition of RPO. Firstly, BC staff use business impact analysis to determine RPO for each service – RPO is not determined by the existent backup regime. Secondly, when any level of preparation of off-site data is required, rather than at the time the backups are offsite, the period during which data is lost very often starts near the time of the beginning of the work to prepare backups which are eventually offsite.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

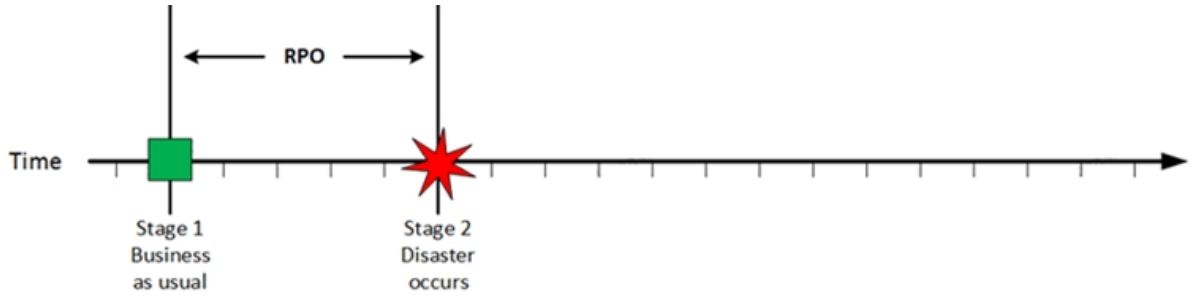
Licensed to Berend Post berend.post@it-university.nl



At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

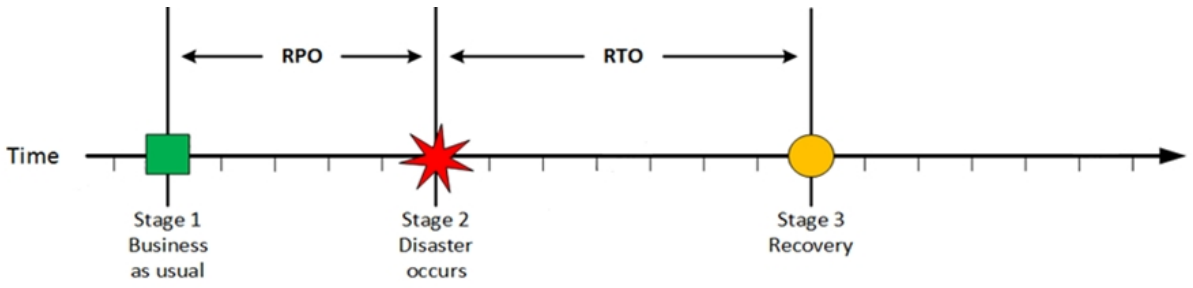
Disaster Occurs



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

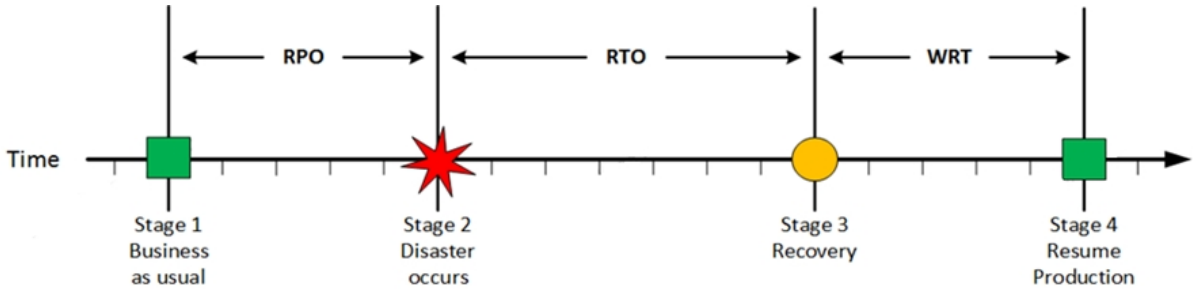


Licensed to Berend Post berend.post@it-university.nl

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.

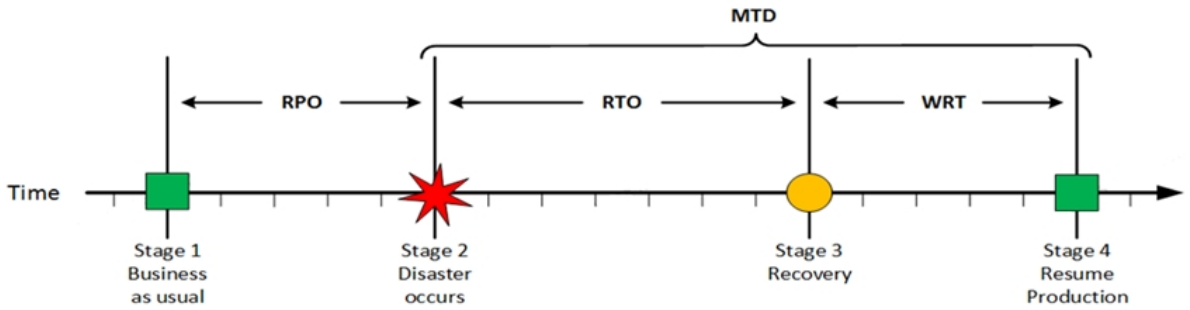
Stage 4: Resume Production

Resume Production



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

Licensed to Berend Post berend.post@it-university.nl

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.

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.

Reference:

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 1565

An advantage of object-oriented system development is that it:

- ☐ partitions systems into a client/server architecture.
- ☐ decreases the need for system documentation.
- ☐ is easier to code than procedural languages.
- ☒ is suited to data with complex relationships.

Licensed to Berend Post berend.post@it-university.nl

Question 1566

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

- ☐ Overall number of users supported
- ☒ Percentage of incidents solved in the first call
- ☐ Number of incidents reported to the help desk
- ☐ Number of agents answering the phones

Explanation:

Explanation:

Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C and D are not quality measures of the help desk service.

Question 1567

Which of the following controls BEST mitigates the impact of a distributed denial of service (DDoS) attack against the controller in a software-defined network (SDN)?

- ☒ Implementing multiple physical SDN controllers
- ☐ Relocating virtualized network functions to physical infrastructure
- ☐ Hardening the operating system that hosts the SDN controller
- ☐ Implementing configuration management for SDN controllers

Question 1568

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- ☐ Halon gas
- ☐ Wet-pipe sprinklers
- ☒ Dry-pipe sprinklers
- ☐ Carbon dioxide gas

Explanation:

Explanation:

Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat to life, and water is environmentally friendly.

Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

Licensed to Berend Post berend.post@it-university.nl

Question 1569

What is the PRIMARY benefit of prototyping as a method of system development?

- ☐ Reduces the need for testing.
- ☐ Minimizes the time the IS auditor has to review the system.
- ☒ Increases the likelihood of user satisfaction.
- ☐ Eliminates the need for documentation.

Question 1570

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

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

Licensed to Berend Post berend.post@it-university.nl

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 account valuation being incorrect because those items are easier to conceal (and therefore easier to steal).

Control Risk

Licensed to Berend Post berend.post@it-university.nl

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 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.

Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

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 1571

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:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

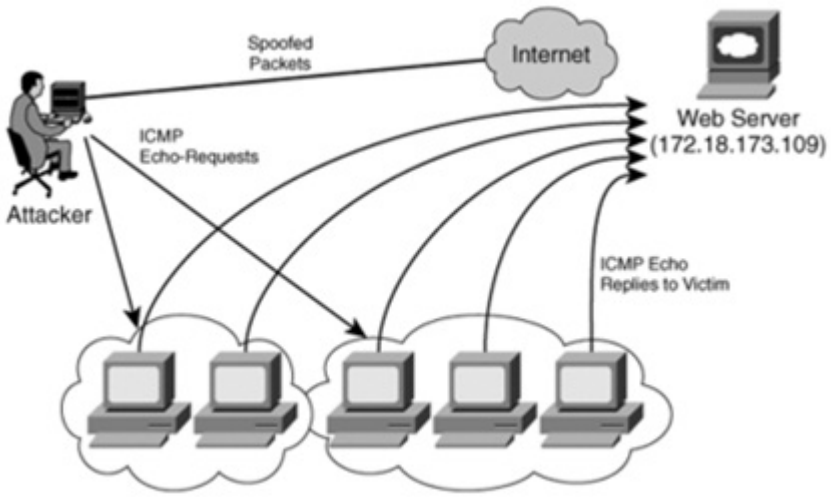
Reflected attack involves sending forged requests to a large number of computers that will reply to the requests. The source IP address is spoofed to that of the targeted victim, causing replies to flood.

A distributed denial of service attack may involve sending forged requests of some type to a very large number of computers that will reply to the requests. Using Internet Protocol address spoofing, the source address is set to that of the targeted victim, which means all the replies will go to (and flood) the target. (This reflected attack form is sometimes called a "DRDOS".

ICMP Echo Request attacks (Smurf Attack) can be considered one form of reflected attack, as the flooding host(s) send Echo Requests to the broadcast addresses of mix-configured networks, thereby enticing hosts to send Echo Reply packets to the victim. Some early DDoS programs implemented a distributed form of this attack.

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:

Licensed to Berend Post berend.post@it-university.nl

Brute force attack - Brute force (also known as brute force cracking) is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Just as a criminal might break into, or "crack" a safe by trying many possible combinations, a brute force cracking application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach.

Buffer overflow - A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity.

Pulsing Zombie - A Dos attack in which a network is subjected to hostile pinging by different attacker computer over an extended time period.

Reference:

CISA review manual 2014 Page number 322

Question 1572

Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

- ☐ virus
- ☐ worm
- ☒ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ None of the choices.

Question 1573

Which of the following would be of MOST concern for an IS auditor evaluating the design of an organization’s incident management processes?

- ☐ Metrics are not reported to senior management.
- ☐ Service management standards are not followed.
- ☐ Expected time to resolve incidents is not specified.
- ☒ Prioritization criteria are not defined.

Licensed to Berend Post berend.post@it-university.nl

Question 1574

An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

- ☒ An application-level gateway
- ☐ A remote access server
- ☐ A proxy server
- ☐ Port scanning

Explanation:

Explanation:

An application-level gateway is the best way to protect against hacking because it can define with detail rules that describe the type of user or connection that is or is not permitted, it analyzes in detail each package, not only in layers one through four of the OSI model but also layers five through seven, which means that it reviews the commands of each higher-level protocol (HTTP, FTP, SNMP, etc.). For a remote access server, there is a device (server) that asks for a username and password before entering the network. This is good when accessing private networks, but it can be mapped or scanned from the Internet creating security exposure. Proxy servers can provide protection based on the IP address and ports. However, an individual is needed who really knows how to do this, and applications can use different ports for the different sections of the program. Port scanning works when there is a very specific task to complete, but not when trying to control what comes from the Internet, or when all the ports available need to be controlled. For example, the port for Ping (echo request) could be blocked and the IP addresses would be available for the application and browsing, but would not respond to Ping.

Question 1575

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 1576

Which of the following areas are the MOST likely cause of an application producing several erroneous reports?

- ☒ A deficiency in user acceptance testing
- ☐ A deficiency in patch management
- ☐ A deficiency in IT resource allocation
- ☐ A deficiency in database administration

Question 1577

With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

- ☒ clarity and simplicity of the business continuity plans.
- ☐ adequacy of the business continuity plans.
- ☐ effectiveness of the business continuity plans.
- ☐ ability of IS and end-user personnel to respond effectively in emergencies.

Explanation:

Explanation:

The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards. To evaluate effectiveness, the IS auditor should review the results from previous tests. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization had implemented plans to allow for the effective response.

Question 1578

Which of the following is critical to the successful establishment of an enterprise IT architecture?

- ☐ A well-defined data migration policy
- ☐ Comparison of the architecture with that of other organizations
- ☐ An architecture encompassing only critical systems
- ☒ Organizational support for standardization

Licensed to Berend Post berend.post@it-university.nl

Question 1579

An IS auditor discovers a recurring software control process issue that severely impacts the efficiency of a critical business process. Which of the following is the BEST recommendation?

- ☐ Replace the malfunctioning system.
- ☐ Determine the compensating controls.
- ☐ Identify other impacted processes.
- ☒ Determine the root cause of the issue.

Question 1580

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.

Question 1581

An organization has an approved bring your own device (BYOD) program. Which of the following is the MOST effective method to enforce application control on personal devices?

- ☒ Implement a mobile device management solution.
- ☐ Establish a mobile device acceptable use policy.
- ☐ Implement a web application firewall.
- ☐ Educate users regarding the use of approved applications.

Question 1582

Which of the following would help to ensure the completeness of batch file transfers?

- ☐ Input controls
- ☐ Self-checking digits
- ☒ Hash totals
- ☐ Parity check

Licensed to Berend Post berend.post@it-university.nl

Question 1583

When migrating critical systems to a cloud provider, the GREATEST data security concern for an organization would be that data from different clients may be:

- ☐ subject to different service level agreements (SLAs) for disaster recovery.
- ☐ subject to varying government compliance regulations.
- ☒ improperly separated from each other.
- ☐ requested during a legal discovery process.

Question 1584

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 1585

An organization is in the process of acquiring a competitor. The information security manager has been asked to report on the security posture of the target acquisition. Which of the following should be the security manager's FIRSTcourse of action?

- ☒ Implement a security dashboard
- ☐ Quantity the potential risk
- ☐ Perform a gap analysis
- ☐ Perform a vulnerability assessment

Question 1586

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:

Licensed to Berend Post berend.post@it-university.nl

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 1587

Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

- ☐ Router
- ☒ Bridge
- ☐ Repeater
- ☐ Gateway

Explanation:

Explanation:

A bridge connects two separate networks to form a logical network (e.g., joining an Ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet.

Question 1588

Establishing the level of acceptable risk is the responsibility of:

- ☐ quality assurance management.
- ☒ senior business management.
- ☐ the chief information officer.
- ☐ the chief security officer.

Explanation:

Explanation:

Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.

Licensed to Berend Post berend.post@it-university.nl

Question 1589

Which of the following is MOST important for an organization to review before sharing data with an external business partner via an application programming interface (API)?

- ☐ The business partner's web application log files
- ☐ The business partner's help desk incident tickets
- ☒ The business partner's security practices
- ☐ The business partner's data center access logs

Question 1590

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 1591

Which of the following would provide the MOST reliable evidence to indicate whether employee access has been deactivated in a timely manner following termination?

- ☐ Comparing termination forms with dates in the HR system
- ☐ Reviewing hardware return-of-asset forms
- ☐ Interviewing supervisors to verify employee data is being updated immediately
- ☒ Comparing termination forms with system transaction log entries

Question 1592

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1593

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 1594

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.

Question 1595

Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

- ☐ RPO
- ☒ RTO
- ☐ WRT
- ☐ MTD

Explanation:

Explanation:

The recovery time objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Licensed to Berend Post berend.post@it-university.nl

It can include the time for trying to fix the problem without a recovery, the recovery itself, testing, and the communication to the users. Decision time for users representative is not included.

The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points.

In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the business continuity planner). The RTOs are then presented to senior management for acceptance.

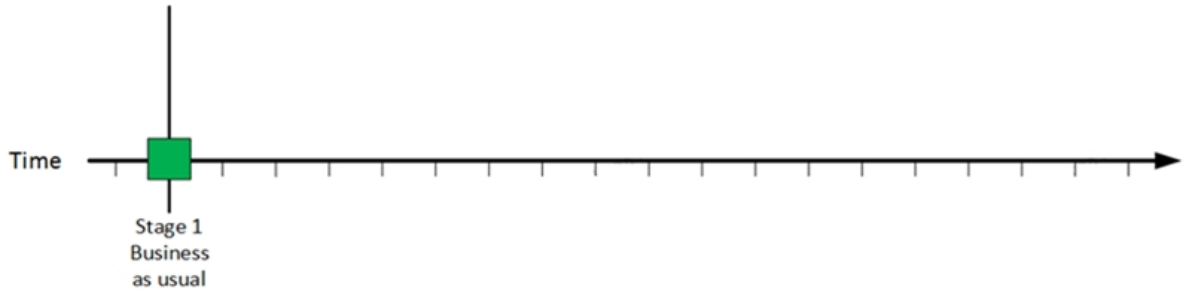
The RTO attaches to the business process and not the resources required to support the process.

The RTO and the results of the BIA in its entirety provide the basis for identifying and analyzing viable strategies for inclusion in the business continuity plan. Viable strategy options would include any which would enable resumption of a business process in a time frame at or near the RTO. This would include alternate or manual workaround procedures and would not necessarily require computer systems to meet the RTOs.

For your exam you should know below information about RPO, RTO, WRT and MTD :

Stage 1: Business as usual

Business as usual

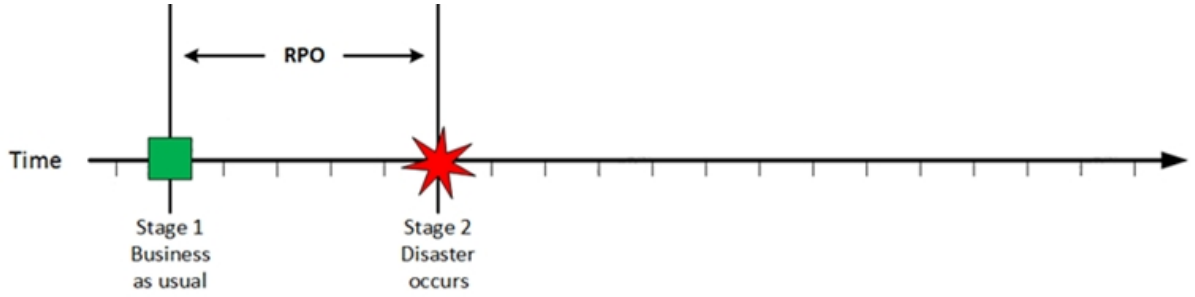


At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

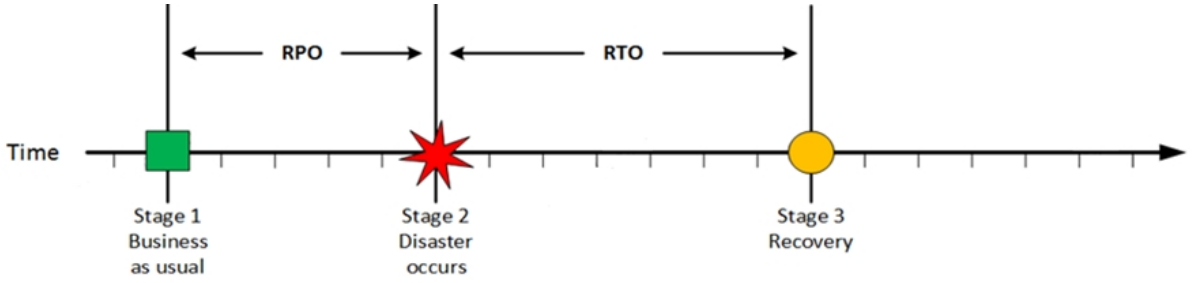
Licensed to Berend Post berend.post@it-university.nl



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

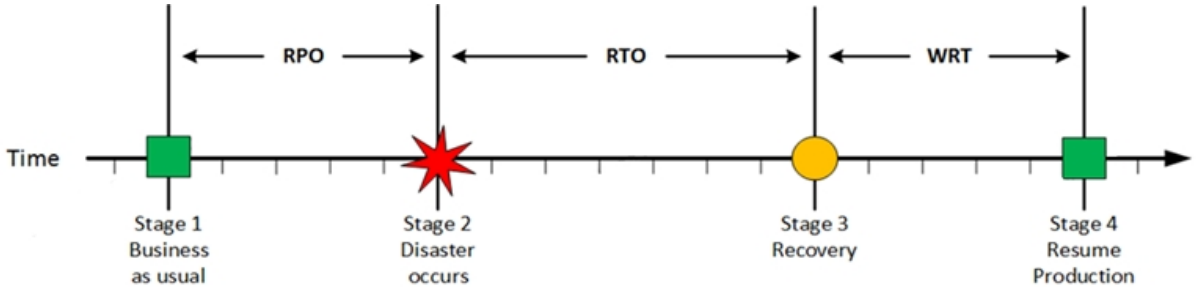
Recovery



At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

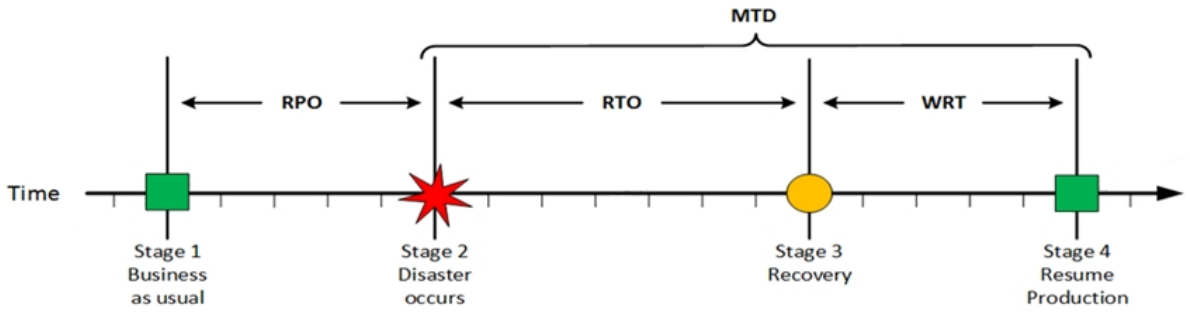
Resume Production



Licensed to Berend Post berend.post@it-university.nl

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

WRT - The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Licensed to Berend Post berend.post@it-university.nl

Reference:

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 1596

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 1597

Properly planned risk-based audit programs are often capable of offering which of the following benefits?

- ☒ audit efficiency and effectiveness.
- ☐ audit efficiency only.
- ☐ audit effectiveness only.
- ☐ audit transparency only.
- ☐ audit transparency and effectiveness.
- ☐ None of the choices.

Explanation:

Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

Licensed to Berend Post berend.post@it-university.nl

Question 1598

Which of the following is the BEST indicator that an application system's agreed-upon level of service has been met?

- ☐ Bandwidth usage logs
- ☒ Transaction response time
- ☐ CPU utilization reports
- ☐ Security incident reports

Question 1599

To ensure message integrity, confidentiality and non-repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

- ☒ the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key by using the receiver's public key.
- ☐ any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering the key using the receiver's public key.
- ☐ the entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key and enciphering both the encrypted message and digest using the receiver's public key.
- ☐ the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Explanation:

Explanation:

Applying a cryptographic hashing algorithm against the entire message addresses the message integrity issue. Enciphering the message digest using the sender's private key addresses non repudiation. Encrypting the message with a symmetric key, thereafter allowing the key to be enciphered using the receiver's public key, most efficiently addresses the confidentiality of the message as well as the receiver's non repudiation. The other choices would address only a portion of the requirements.

Licensed to Berend Post berend.post@it-university.nl

Question 1600

Which of the following helps to ensure the integrity of data for an interface between a new billing system and an accounts receivable system?

- ☐ Audit logs are available for 30 days.
- ☐ Access to the data requires authentication.
- ☐ Data files are encrypted during transmission.
- ☒ Control totals are calculated.

Question 1601

During a follow-up audit, an IS auditor learns the organization implemented an automated process instead of the originally agreed upon enhancement of the manual process. The auditor should:

- ☐ report the finding that recommendations were not acted upon
- ☐ perform a cost-benefit analysis on the new process
- ☒ verify that the new process satisfies control objectives
- ☐ report the recommendation as implemented

Question 1602

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 1603

Which of the following is MOST likely to enable a hacker to successfully penetrate a system?

- ☐ Lack of virus protection
- ☒ Unpatched software
- ☐ Decentralized dialup access
- ☐ Lack of DoS protection

Licensed to Berend Post berend.post@it-university.nl

Question 1604

During the extraction and transfer process of data from an application database to an enterprise data warehouse, some of the fields were not picked up in the extraction process and therefore did not end up in the data warehouse. Which of the following is the GREATEST concern with this situation?

- ☐ Costs associated with correcting the process may exceed budget
- ☒ Transaction errors may occur within the application
- ☐ Management decisions may be based on incorrect data
- ☐ Management reporting could be delayed

Question 1605

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 1606

Which of the following is an effective way to ensure the integrity of file transfers in a peer-to-peer (P2P) computing environment?

- ☐ Connect the client computers in the environment to a jump server.
- ☐ Ensure the files transferred through an intrusion detection system (IDS).
- ☐ Encrypt the packets shared between peers within the environment.
- ☒ Associate a message authentication code with each file transferred.

Question 1607

The BEST way to validate whether a malicious act has actually occurred in an application is to review:

- ☐ segregation of duties
- ☐ access controls
- ☒ activity logs
- ☐ change management logs

Licensed to Berend Post berend.post@it-university.nl

Question 1608

Which of the following would BEST provide executive management with current information on IT-related costs and IT performance indicators?

- ☒ IT dashboard
- ☐ Risk register
- ☐ IT service-management plan
- ☐ Continuous audit reports

Question 1609

An employee loses a mobile device resulting in loss of sensitive corporate data. Which of the following would have BEST prevented data leakage?

- ☐ Awareness training for mobile device users
- ☐ Data encryption on the mobile device
- ☒ The triggering of remote data wipe capabilities
- ☐ Complex password policy for mobile devices

Question 1610

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- ☐ the existing IT environment.
- ☒ the business plan.
- ☐ the present IT budget.
- ☐ current technology trends.

Explanation:

Explanation:

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

Question 1611

Business applications should be selected for disaster recovery testing on the basis of:

- ☐ the results of contingency desktop checks
- ☐ the number of failure points that are being tested
- ☒ recovery time objectives (RTOs)
- ☐ criticality to the enterprise

Licensed to Berend Post berend.post@it-university.nl

Question 1612

Which of the following layer from an enterprise data flow architecture captures all data of interest to an organization and organize it to assist in reporting and analysis?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☒ Core data warehouse
- ☐ Data access layer

Explanation:

Explanation:

Core data warehouse – This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance.

To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer – Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

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 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.

Reference:

CISA review manual 2014 Page number 188

Question 1613

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.

Question 1614

During a follow-up audit, an IS auditor finds that some critical recommendations have not been addressed as management has decided to accept the risk. Which of the following is the IS auditor's BEST course of action?

- ☐ Adjust the annual risk assessment accordingly.
- ☐ Require the auditee to address the recommendations in full.
- ☒ Evaluate senior management's acceptance of the risk.
- ☐ Update the audit program based on management's acceptance of risk.

Licensed to Berend Post berend.post@it-university.nl

Question 1615

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.

Question 1616

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.

Question 1617

The MOST likely explanation for a successful social engineering attack is:

- ☐ that computers make logic errors.
- ☒ that people make judgment errors.
- ☐ the computer knowledge of the attackers.
- ☐ the technological sophistication of the attack method.

Explanation:

Explanation:

Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

Licensed to Berend Post berend.post@it-university.nl

Question 1618

An audit group is conducting a risk assessment as part of a risk-based audit strategy. To help ensure the risk assessment results are relevant to the organization, it is MOST important to:

- ☒ understand the organization's objectives and risk appetite.
- ☐ include operational departments and processes.
- ☐ determine both the inherent risk and detection risk.
- ☐ understand the organization's controls.

Question 1619

Which of the following would BEST enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy?

- ☐ Mobile device upgrade program
- ☐ Mobile device tracking program
- ☒ Mobile device awareness program
- ☐ Mobile device testing program

Question 1620

The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?

- ☐ Rewrite the patches and apply them
- ☐ Code review and application of available patches
- ☐ Develop in-house patches
- ☒ identify and test suitable patches before applying them

Explanation:

Explanation:

Suitable patches from the existing developers should be selected and tested before applying them. Rewriting the patches and applying them is not a correct answer because it would require skilled resources and time to rewrite the patches. Code review could be possible but tests need to be performed before applying the patches. Since the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.

Licensed to Berend Post berend.post@it-university.nl

Question 1621

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 1622

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.

Question 1623

During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

- ☐ responsibility for maintaining the business continuity plan.
- ☐ criteria for selecting a recovery site provider.
- ☒ recovery strategy.
- ☐ responsibilities of key personnel.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The most appropriate strategy is selected based on the relative risk level and criticality identified in the business impact analysis (BIA.) The other choices are made after the selection or design of the appropriate recovery strategy.

Question 1624

Which of the following should an IS auditor review FIRST when planning a customer data privacy audit?

- ☐ Legal and compliance requirements
- ☒ Customer agreements
- ☐ Organizational policies and procedures
- ☐ Data classification

Question 1625

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.

Question 1626

To help ensure the organization's information assets are adequately protected, which of the following considerations is MOST important when developing an information classification and handling policy?

- ☐ The policy has been mapped against industry frameworks for classifying information assets.
- ☐ The policy is owned by the head of information security, who has the authority to enforce the policy.
- ☐ The policy specifies requirements to safeguard information assets based on their importance to the organization.
- ☒ The policy is subject to periodic reviews to ensure its provisions are up to date.

Licensed to Berend Post berend.post@it-university.nl

Question 1627

The BEST way for an IS auditor to determine which business processes are currently outsourced to a specific service provider is to review the:

- ☐ enterprise architecture (EA) diagram.
- ☒ service provider's contract.
- ☐ vendor management policy.
- ☐ request for proposal (RFP) responses.

Question 1628

The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

- ☐ prevent omission or duplication of transactions.
- ☐ ensure smooth data transition from client machines to servers.
- ☐ ensure that e-mail messages have accurate time stamps.
- ☒ support the incident investigation process.

Explanation:

Explanation:

During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult because a time line of events might not be easily established. Time-stamping a transaction has nothing to do with the update itself. Therefore, the possibility of omission or duplication of transactions does not exist. Data transfer has nothing to do with the time stamp. While the time stamp on an e-mail may not be accurate, this is not a significant issue.

Question 1629

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 1630

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 1631

E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

- ☒ sender's private key and encrypting the message using the receiver's public key.
- ☐ sender's public key and encrypting the message using the receiver's private key.
- ☐ receiver's private key and encrypting the message using the sender's public key.
- ☐ receiver's public key and encrypting the message using the sender's private key.

Explanation:

Explanation:

By signing the message with the sender's private key, the receiver can verify its authenticity using the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt the message using their own private key. The receiver's private key is confidential and, therefore, unknown to the sender. Messages encrypted using the sender's private key can be read by anyone with the sender's public key.

Question 1632

Which of the following BEST helps to identify errors during data transfer?

- ☐ Decrease the size of data transfer packets.
- ☒ Test the integrity of the data transfer.
- ☐ Review and verify the data transfer sequence numbers.
- ☐ Enable a logging process for data transfer.

Question 1633

In the review of a feasibility study for an IS acquisition, the MOST important step is to:

- ☐ determine whether the cost-benefits are achievable.
- ☐ ensure that a contingency plan is in place should the project fail.
- ☐ ensure that the right to audit the vendor has been considered.
- ☒ determine whether security and control requirements have been specified.

Question 1634

Reviewing project plans and status reports throughout the development life cycle will:

- ☐ eliminate the need to perform a risk assessment.
- ☐ postpone documenting the project's progress until the final phase.
- ☐ guarantee that the project will meet its intended deliverables.
- ☒ facilitate the optimal use of resources over the life of the project.

Licensed to Berend Post berend.post@it-university.nl

Question 1635

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 1636

Which of the following must exist to ensure the viability of a duplicate information processing facility?

- ☐ The site is near the primary site to ensure quick and efficient recovery.
- ☐ The site contains the most advanced hardware available.
- ☒ The workload of the primary site is monitored to ensure adequate backup is available.
- ☐ The hardware is tested when it is installed to ensure it is working properly.

Explanation:

Explanation:

Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure the operation will continue to perform as planned.

Licensed to Berend Post berend.post@it-university.nl

Question 1637

Which of the following roles is ULTIMATELY accountable for the protection of an organization's information?

- ☐ The board of directors
- ☐ The chief information security officer (CISO)
- ☒ The data owner
- ☐ The chief information officer (CIO)

Question 1638

During an investigation of transactions in a core banking system, fraudulent transactions are discovered that will require the involvement of law enforcement. Which of the following should be done FIRST?

- ☐ Ensure evidence is preserved.
- ☒ Initiate incident response procedures.
- ☐ Evaluate the business impact.
- ☐ Notify internal audit management.

Question 1639

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1640

Which of the following is protocol data unit (PDU) of network interface layer in TCP/IP model?

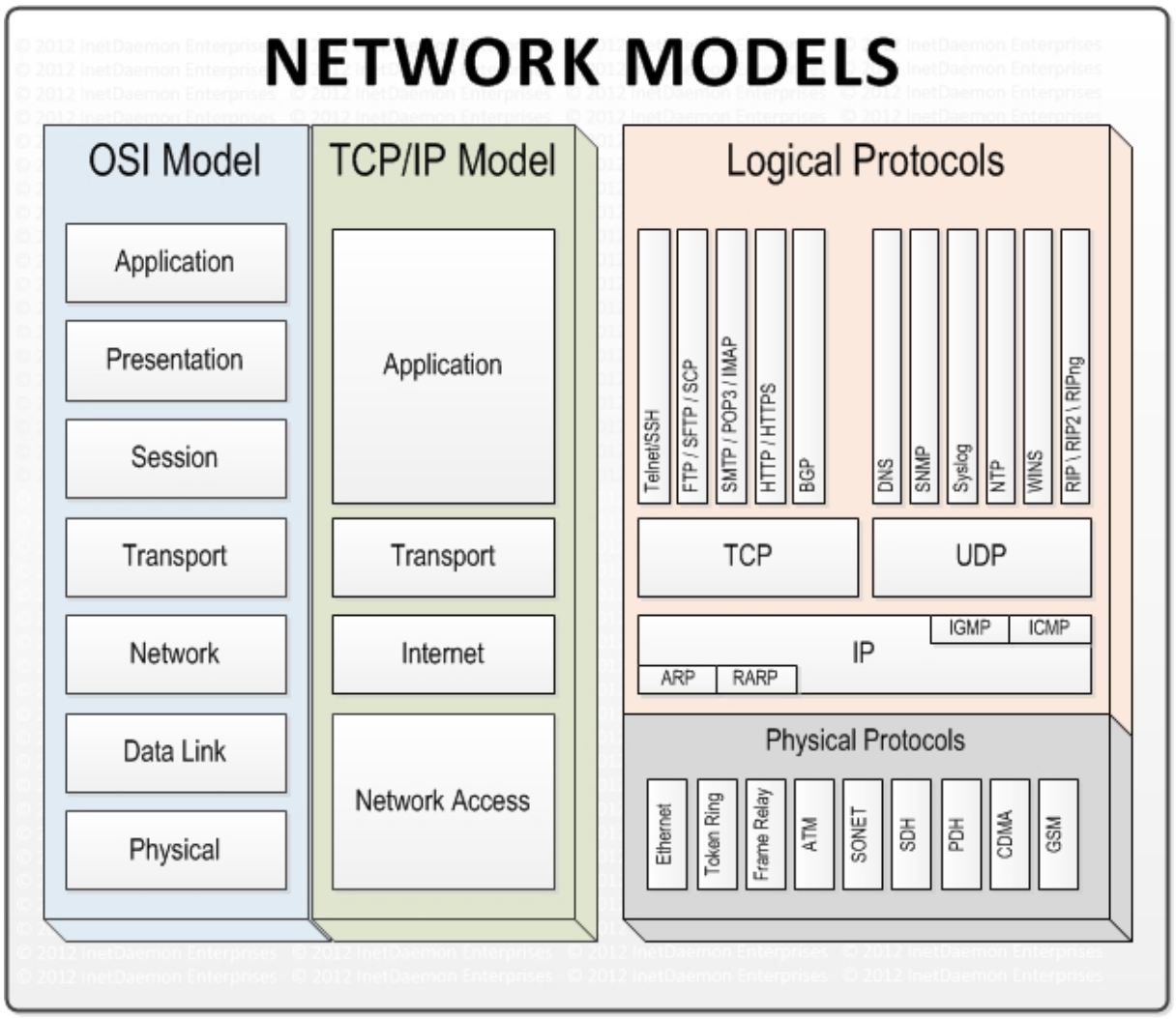
- ☐ Data
- ☐ Segment
- ☒ Packet
- ☐ Frame

Explanation:

Explanation:

For your exam you should know below information about TCP/IP model:

Network models



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Licensed to Berend Post berend.post@it-university.nl

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

The main protocols included at Transport layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Layer 2. Internet Layer

Internet Layer is the second layer of the four layer TCP/IP model. The position of Internet layer is between Network Access Layer and Transport layer. Internet layer pack data into data packets known as IP datagram's, which contain source and destination address (logical address or IP address) information that is used to forward the datagram's between hosts and across networks. The Internet layer is also responsible for routing of IP datagram's.

Packet switching network depends upon a connectionless internetwork layer. This layer is known as Internet layer. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. At the destination side data packets may appear in a different order than they were sent. It is the job of the higher layers to rearrange them in order to deliver them to proper network applications operating at the Application layer.

The main protocols included at Internet layer are IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol) and IGMP (Internet Group Management Protocol).

Layer 1. Network Access Layer

Network Access Layer is the first layer of the four layer TCP/IP model. Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.

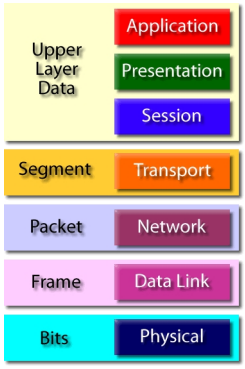
The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame Relay etc.

Licensed to Berend Post berend.post@it-university.nl

The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

IN CSMA/CD Access Method, every host has equal access to the medium and can place data on the wire when the wire is free from network traffic. When a host wants to place data on the wire, it will check the wire to find whether another host is already using the medium. If there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted.

Protocol Data Unit (PDU):



The following answers are incorrect:

Data – Application layer PDU

Segment – Transport layer PDU

Frame/bit – LAN or WAN interface layer PDU

Reference:

CISA review manual 2014 page number 272

Licensed to Berend Post berend.post@it-university.nl

Question 1641

After assessing risk, the decision to treat the risk should be based PRIMARILY on:

- ☐ whether the level of risk exceeds risk appetite
- ☐ availability of financial resources
- ☐ whether the level of risk exceeds inherent risk
- ☒ the criticality of the risk

Question 1642

What can be implemented to provide the highest level of protection from external attack?

- ☒ Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- ☐ Configuring the firewall as a screened host behind a router
- ☐ Configuring the firewall as the protecting bastion host
- ☐ Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Explanation:

Explanation:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

Question 1643

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

Licensed to Berend Post berend.post@it-university.nl

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.

Question 1644

A payroll application system accepts individual user sign-on IDs and then connects to its database using a single application ID. The GREATEST weakness under this system architecture is that:

- ☐ an incident involving unauthorized access to data cannot be tied to a specific user.
- ☐ when multiple sessions with the same application ID collide, the database locks up.
- ☒ users can gain direct access to the application ID and circumvent data controls.
- ☐ the database becomes unavailable if the password of the application ID expires.

Question 1645

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 1646

Which of the following layer in an enterprise data flow architecture derives enterprise information from operational data, external data and nonoperational data?

- ☐ Data preparation layer
- ☒ Data source layer
- ☐ Data mart layer
- ☐ Data access layer

Explanation:

Explanation:

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.

For CISA exam you should know below information about business intelligence:

Business intelligence(BI) is a broad field of IT encompasses the collection and analysis of information to assist decision making and assess organizational performance. To deliver effective BI, organizations need to design and implement a data architecture. The complete data architecture consists of two components

The enterprise data flow architecture (EDFA)

A logical data architecture

Various layers/components of this data flow architecture are as follows:

Presentation/desktop access layer – This is where end users directly deal with information. This layer includes familiar desktop tools such as spreadsheets, direct querying tools, reporting and analysis suits offered by vendors such as Congas and business objects, and purpose built application such as balanced source cards and digital dashboards.

Data Source Layer - Enterprise information derives from number of sources:

Operational data – Data captured and maintained by an organization's existing systems, and usually held in system-specific database or flat files.

External Data – Data provided to an organization by external sources. This could include data such as customer demographic and market share information.

Nonoperational data – Information needed by end user that is not currently maintained in a computer accessible format.

 Licensed to Berend Post berend.post@it-university.nl

Core data warehouse -This is where all the data of interest to an organization is captured and organized to assist reporting and analysis. DWs are normally instituted as large relational databases. A property constituted DW should support three basic form of an inquiry.

Drilling up and drilling down – Using dimension of interest to the business, it should be possible to aggregate data as well as drill down. Attributes available at the more granular levels of the warehouse can also be used to refine the analysis.

Drill across – Use common attributes to access a cross section of information in the warehouse such as sum sales across all product lines by customer and group of customers according to length of association with the company.

Historical Analysis – The warehouse should support this by holding historical, time variant data. An example of historical analysis would be to report monthly store sales and then repeat the analysis using only customer who were preexisting at the start of the year in order to separate the effective new customer from the ability to generate repeat business with existing customers.

Data Mart Layer- Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data Staging and quality layer -This layer is responsible for data copying, transformation into DW format and quality control. It is particularly important that only reliable data into core DW. This layer needs to be able to deal with problems periodically thrown by operational systems such as change to account number format and reuse of old accounts and customer numbers.

Data Access Layer -This layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data Preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed. Data mining is concern with exploring large volume of data to determine patterns and trends of information. Data mining often identifies patterns that are counterintuitive due to number and complexity of data relationships. Data quality needs to be very high to not corrupt the result.

Metadata repository layer - Metadata are data about data. The information held in metadata layer needs to extend beyond data structure names and formats to provide detail on business purpose and

Licensed to Berend Post berend.post@it-university.nl

context. The metadata layer should be comprehensive in scope, covering data as they flow between the various layers, including documenting transformation and validation rules.

Warehouse Management Layer -The function of this layer is the scheduling of the tasks necessary to build and maintain the DW and populate data marts. This layer is also involved in administration of security.

Application messaging layer -This layer is concerned with transporting information between the various layers. In addition to business data, this layer encompasses generation, storage and targeted communication of control messages.

Internet/Intranet layer – This layer is concerned with basic data communication. Included here are browser based user interface and TCP/IP networking.

Various analysis models used by data architects/ analysis follows:

Activity or swim-lane diagram – De-construct business processes.

Entity relationship diagram -Depict data entities and how they relate. These data analysis methods obviously play an important part in developing an enterprise data model. However, it is also crucial that knowledgeable business operative is involved in the process. This way proper understanding can be obtained of the business purpose and context of the data. This also mitigates the risk of replication of suboptimal data configuration from existing systems and database into DW.

The following were incorrect answers:

Data mart layer - Data mart represents subset of information from the core DW selected and organized to meet the needs of a particular business unit or business line. Data mart can be relational databases or some form on-line analytical processing (OLAP) data structure.

Data access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Licensed to Berend Post berend.post@it-university.nl

Reference:

CISA review manual 2014 Page number 188

Question 1647

Which of the following key performance indicators (KPIs) provides the BEST indication of a security awareness campaign's effectiveness?

- ☐ Reduced average time for incident resolution
- ☐ Percentage of attendees passing the awareness quiz
- ☐ Decrease in the number of help desk calls
- ☒ Increase in the number of reported security incidents

Question 1648

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 1649

Which of the following should be the PRIMARY consideration when developing an IT strategy?

- ☐ IT key performance indicators based on business objectives
- ☒ Alignment with overall business objectives
- ☐ Alignment with the IT investment portfolio
- ☐ Short and long-term plans for the enterprise IT architecture

Question 1650

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1651

An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

- ☒ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Explanation:

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need. A warm site is an offsite backup facility that is partially configured with network connections and selected peripheral equipment-such as disk and tape units, controllers and CPUs-to operate an information processing facility. A duplicate information processing facility is a dedicated, self-developed recovery site that can back up critical applications.

Question 1652

Which of the following reports should an IS auditor use to check compliance with a service level agreements (SLA) requirement for uptime?

- ☐ Utilization reports
- ☐ Hardware error reports
- ☐ System logs
- ☒ Availability reports

Explanation:

Explanation:

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

Question 1653

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:

Licensed to Berend Post berend.post@it-university.nl

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.

Question 1654

Which of the following is MOST critical for the effective implementation of IT governance?

- ☐ Internal auditor commitment
- ☒ Supportive corporate culture
- ☐ Strong risk management practices
- ☐ Documented policies

Question 1655

The BEST method an organization can employ to align its business continuity plan (BCP) and disaster recovery plan (DRP) with core business needs is to:

- ☐ execute periodic walk-throughs of the plans.
- ☒ update the business impact analysis (BIA) for significant business changes.
- ☐ outsource the maintenance of the BCP and disaster recovery plan to a third party.
- ☐ include BCP and disaster recovery plan responsibilities as a part of new employee training.

Question 1656

Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

- ☐ Multiplexer
- ☒ Modem
- ☐ Protocol converter
- ☐ Concentrator

Explanation:

Explanation:

A modem is a device that translates data from digital to analog and back to digital.

Licensed to Berend Post berend.post@it-university.nl

Question 1657

An IS auditor is assessing an organization's implementation of a virtual network. Which of the following observations should be considered the MOST significant risk?

- ☐ Communication performance over the virtual network is not monitored.
- ☐ Virtual network devices are replicated and stored in offline mode.
- ☒ Traffic over the virtual network is not visible to security protection devices.
- ☐ Physical and virtual network configurations are not managed by the same team.

Question 1658

An organization's IT department is undertaking a large virtualization project to reduce its physical server footprint. Which of the following should be the HIGHEST priority of the information security manager?

- ☐ Determining how incidents will be managed
- ☐ Selecting the virtualization software
- ☒ Being involved as the design stage of the project
- ☐ Ensuring the project has appropriate security funding

Question 1659

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- ☒ a clear business case has been approved by management.
- ☐ corporate security standards will be met.
- ☐ users will be involved in the implementation plan.
- ☐ the new system will meet all required user functionality.

Explanation:

Explanation:

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditor's first concern.

Licensed to Berend Post berend.post@it-university.nl

Question 1660

Which of the following fourth generation language depends on self-contained database management systems?

- ☐ Query and report generator
- ☒ Embedded database 4GLs
- ☐ Relational database 4GL
- ☐ Application generators

Explanation:

Explanation:

Embedded database 4GLsare depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

For CISA exam you should know below mentioned types of 4GLs

Query and report generator – These specialize language can extract and produce reports. Recently more powerful language has been produced that can access database records, produce complex on-line output and be developed in an almost natural language.

Embedded database 4GLs – These depend on self-contained database management systems. These characteristics often makes them more user-friendly but also may lead to applications that are not integrated well with other product applications. Example includes FOCUS, RAMIS II and NOMAD 2.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line. These allow the application developer to make better use of DBMS product, but they often are not end-user-oriented. Example include SQL+ MANTIS and NATURAL.

Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C. The application can be further tailored and customized. Data processing development personnel, not end user, use application generators.

The following were incorrect answers:

Query and report generator – These specialize language can extract and produce reports.

Relational database 4GLs – These high level language products are usually an optional feature on vendor's DBMS product line.

Licensed to Berend Post berend.post@it-university.nl

Application generators – These development tools generate lower level programming languages(3GL) such as COBOL and C.

Reference:

CISA review manual 2014 Page number 209

Question 1661

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

- ☐ DES
- ☒ AES
- ☐ Triple DES
- ☐ RSA

Explanation:

Explanation:

Advanced Encryption Standard (AES), a public algorithm that supports keys from 128 to 256 bits in size, not only provides good security, but provides speed and versatility across a variety of computer platforms. AES runs securely and efficiently on large computers, desktop computers and even small devices such as smart cards. DES is not considered a strong cryptographic solution since its entire key space can be brute forced by large computer systems within a relatively short period of time. Triple DES can take up to three times longer than DES to perform encryption and decryption. RSA keys are large numbers that are suitable only for short messages, such as the creation of a digital signature.

Question 1662

The most common problem in the operation of an intrusion detection system (IDS) is:

- ☒ the detection of false positives.
- ☐ receiving trap messages.
- ☐ reject-error rates.
- ☐ denial-of-service attacks.

Explanation:

Explanation:

Because of the configuration and the way IDS technology operates, the main problem in operating IDSs is the recognition (detection) of events that are not really security incidents- false positives, the equivalent of a false alarm. An IS auditor needs to be aware of this and should check for implementation of related controls, such as IDS tuning, and incident handling procedures, such as the screening process to know if an event is a security incident or a false positive. Trap messages are

 Licensed to Berend Post berend.post@it-university.nl

generated by the Simple Network Management Protocol (SNMP) agents when an important event happens, but are not particularly related to security or IDSs.

Reject-error rate is related to biometric technology and is not related to IDSs. Denial-of-service is a type of attack and is not a problem in the operation of IDSs.

Question 1663

Which of the following cloud deployment models would BEST meet the needs of a startup software development organization with limited initial capital?

- ☐ Private
- ☒ Public
- ☐ Community
- ☐ Hybrid

Question 1664

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:

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.

Data Acquisition – All information and data required should transferred into a controlled location; this includes all types of electronic media such as fixed disk drives and removable media. Each device

Licensed to Berend Post berend.post@it-university.nl

must be checked to ensure that it is write protected. This may be achieved by using device known as write blocker.

Imaging -The Imaging is a process that allows one to obtain bit-for bit copy of a data to avoid damage of original data or information when multiple analyses may be performed. The imaging process is made to obtain residual data, such as deleted files, fragments of deleted files and other information present, from the disk for analysis. This is possible because imaging duplicates the disk surface, sector by sector.

Extraction - This process consists of identification and selection of data from the imaged data set. This process should include standards of quality, integrity and reliability. The extraction process includes software used and media where an image was made. The extraction process could include different sources such as system logs, firewall logs, audit trails and network management information.

Interrogation -Integration is used to obtain prior indicators or relationships, including telephone numbers, IP addresses, and names of individuals from extracted data.

Investigation/ Normalization -This process converts the information extracted to a format that can be understood by investigator. It includes conversion of hexadecimal or binary data into readable characters or a format suitable for data analysis tool.

Reporting- The information obtained from computer forensic has limited value when it is not collected and reported in proper way. When an IS auditor writes report, he/she must include why the system was reviewed, how the computer data were reviewed and what conclusion were made from analysis. The report should achieve the following goals

Accurately describes the details of an incident.

Be understandable to decision makers.

Be able to withstand a barrage of legal security

Be unambiguous and not open to misinterpretation.

Be easily referenced

Contains all information required to explain conclusions reached

Offer valid conclusions, opinions or recommendations when needed

Be created in timely manner.

Licensed to Berend Post berend.post@it-university.nl

The following were incorrect answers:

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.

Reference:

CISA review manual 2014 Page number367 and 368

Question 1665

A company converted its payroll system from an external service to an internal package. Payroll processing in April was run in parallel. To validate the completeness of data after the conversion, which of the following comparisons from the old to the new system would be MOST effective?

- ☐ Turnaround time for payroll processing
- ☐ Employee counts and year-to-date payroll totals
- ☒ Master file employee data to payroll journals
- ☐ Cut-off dates and overwrites for a sample of employees

Question 1666

The application systems quality assurance (QA) function should:

- ☐ assist programmers in designing and developing applications.
- ☐ design and develop quality applications by employing system development methodology.
- ☐ compare programs to approved system changes.
- ☒ ensure adherence of programs to standards.

Licensed to Berend Post berend.post@it-university.nl

Question 1667

Which of the following are BEST suited for continuous auditing?

- ☐ Manual transactions
- ☐ Irregular transactions
- ☐ Low-value transactions
- ☒ Real-time transactions

Question 1668

Capacity management enables organizations to:

- ☐ establish the capacity of network communication links.
- ☐ determine business transaction volumes.
- ☐ forecast technology trends.
- ☒ identify the extent to which components need to be upgraded.

Question 1669

An IS auditor is reviewing documentation of application systems change control and identifies several patches that were not tested before being put into production. Which of the following is the MOST significant risk from this situation?

- ☐ Developer access to production
- ☐ Lack of system integrity
- ☐ Outdated system documentation
- ☒ Loss of application support

Question 1670

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:

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:

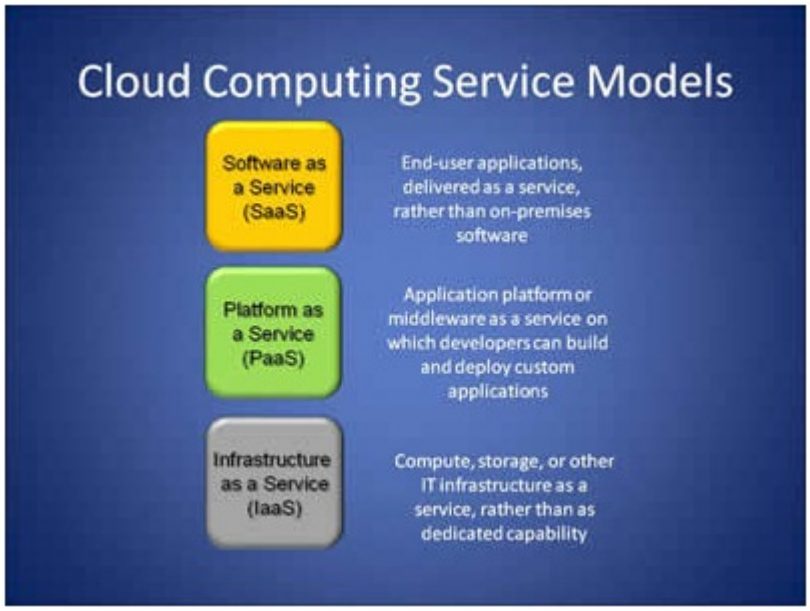
Licensed to Berend Post berend.post@it-university.nl

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.

Reference:

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 1671

Performance of a biometric measure is usually referred to in terms of (Choose three.):

- ☐ failure to reject rate
- ☒ false accept rate
- ☒ false reject rate
- ☒ failure to enroll rate
- ☐ None of the choices.

Explanation:

Explanation:

Performance of a biometric measure is usually referred to in terms of the false accept rate (FAR), the false non match or reject rate (FRR), and the failure to enroll rate (FTE or FER). The FAR measures the percent of invalid users who are incorrectly accepted in, while the FRR measures the percent of valid users who are wrongly rejected.

Question 1672

Which of the following is NOT an example of preventive control?

- ☐ Physical access control like locks and door
- ☐ User login screen which allows only authorize user to access website
- ☒ Encrypt the data so that only authorize user can view the same
- ☐ Duplicate checking of a calculations

Explanation:

Explanation:

The word NOT is used as a keyword in the question. You need to find out a security control from given options which in not preventive. Duplicate checking of a calculation is a detective control and not a preventive control.

For your exam you should know below information about different security controls

Deterrent Controls

Deterrent Controls are intended to discourage a potential attacker. Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some

 Licensed to Berend Post berend.post@it-university.nl

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 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

 Licensed to Berend Post berend.post@it-university.nl

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 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,

Licensed to Berend Post berend.post@it-university.nl

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

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

 Licensed to Berend Post berend.post@it-university.nl

system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk.

For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol, can be employed and layered on top of the authentication process to support the policy statement.

Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk.

As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system.

This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Licensed to Berend Post berend.post@it-university.nl

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management.

Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install.

Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

The following answers are incorrect:

The other examples belong to Preventive control.

Reference:

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 1673

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.

Question 1674

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 1675

Which of the following controls MOST effectively reduces the risk associated with use of instant messaging (IM) in the workplace?

- ☐ Traffic encryption
- ☐ Session border controllers
- ☐ Network address translation
- ☒ Blocking peer-to-peer (P2P) clients

Licensed to Berend Post berend.post@it-university.nl

Question 1676

At which stage of the software development life cycle should an organization identity privacy considerations?

- ☐ Design
- ☐ Testing
- ☐ Development
- ☒ Requirements

Question 1677

When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

When participating in a systems-development project, an IS auditor should also strive to ensure that adequate and complete documentation exists for all projects.

Question 1678

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 1679

A data breach has occurred at a third-party vendor used by an organization to outsource the processing of its customer data. What should be management's FIRST course of action?

- ☐ Activate the disaster recovery plan
- ☐ Notify the insurance company of the potential claim
- ☒ Activate the incident management process
- ☐ Take legal action against the service provider for reputation damage

Licensed to Berend Post berend.post@it-university.nl

Question 1680

Which type of risk would MOST influence the selection of a sampling methodology?

- ☐ Control
- ☐ Inherent
- ☐ Residual
- ☒ Detection

Question 1681

Which of the following entities is BEST suited to define the data classification levels within an organization?

- ☐ Database administrator based on the data schema
- ☐ Legal compliance team based on the application regulations
- ☒ Business owner responsible for the respective data
- ☐ System administrator responsible for data security controls

Question 1682

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1683

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

- ☐ Nonconnection-oriented protocols
- ☒ Connection-oriented protocols
- ☐ Session-oriented protocols
- ☐ Nonsession-oriented protocols

Explanation:

Explanation:

The transport layer of the TCP/IP protocol suite provides for connection- oriented protocols to ensure reliable communication.

Question 1684

Following a recent internal data breach, an IS auditor was asked to evaluate information security practices within the organization. Which of the following findings would be MOST important to report to senior management?

- ☐ Employees are not required to sign a non-compete agreement.
- ☐ Security education and awareness workshops have not been completed.
- ☒ Users lack technical knowledge related to security and data protection.
- ☐ Desktop passwords do not require special characters.

Question 1685

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 1686

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

Licensed to Berend Post berend.post@it-university.nl

Question 1687

In assessing the priority given to systems covered in an organization's business continuity plan (BCP), an IS auditor should FIRST:

- ☐ review results of previous business continuity plan (BCP) tests.
- ☐ review the backup and restore processes.
- ☐ verify the criteria for disaster recovery site selection.
- ☒ validate the recovery time objectives and recovery point objectives.

Question 1688

Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?

- ☒ Three users with the ability to capture and verify their own messages
- ☐ Five users with the ability to capture and send their own messages
- ☐ Five users with the ability to verify other users and to send their own messages
- ☐ Three users with the ability to capture and verify the messages of other users and to send their own messages

Explanation:

Explanation:

The ability of one individual to capture and verify messages represents an inadequate segregation, since messages can be taken as correct and as if they had already been verified.

Question 1689

Which of the following BEST enables timely detection of changes in the IT environment to support informed decision making by management?

- ☒ Continuous monitoring
- ☐ Sampling checks on high-risk areas
- ☐ Change management reports
- ☐ Established key risk indicators (KRIs)

Question 1690

As an IS auditor, it is very important to make sure all storage media are well protected. Which of the following is the LEAST important factor for protecting CDs and DVDs?

- ☐ Handle by edges or by the hole in the middle
- ☒ Store in anti-static bag
- ☐ Avoid long term exposure to bright light
- ☐ Store in a hard jewel case, not in soft sleeves

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

CDs and DVDs are least affected by static current so it is not as important to store them into anti-static bags.

CDs and DVDs Storage protection recommendations:

Handle by edges or by hole in the middle

Be careful not to bend the CD or DVD

Avoid long term exposure to bright light

Store in a hard jewel case, not is soft sleeves

Also, you should know the media storage precautions listed below in preparation for the CISA exam:

USB and portable hard drive

Avoid high temperature, humidity extremes and strong magnetic field

Tape Cartridges

Store Cartridges vertically

Store cartridges in a protective container for transport

Write-protect cartridges immediately

Hard Drive

Store hard drives in anti-static bags, and be sure that person removing them from bag is static free

If the original box and padding for the hard drive is available, use it for shipping

If the hard drive has been in a cold environment, bring it to room temperature prior to installing and using it

Reference:

Reference used - CISA review manual 2014. Page number 338

Licensed to Berend Post berend.post@it-university.nl

Question 1691

Which of the following occurs during the issues management process for a system development project?

- ☐ Contingency planning
- ☐ Impact assessment
- ☐ Configuration management
- ☒ Help desk management

Question 1692

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 1693

The quality of the metadata produced from a data warehouse is _____ in the warehouse's design.

- ☐ Often hard to determine because the data is derived from a heterogeneous data environment
- ☒ The most important consideration
- ☐ Independent of the quality of the warehoused databases
- ☐ Of secondary importance to data warehouse content

Explanation:

Explanation:

The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

Question 1694

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:

Licensed to Berend Post berend.post@it-university.nl

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 1695

Which of the following should be the MOST important consideration in IT portfolio management?

- ☒ Aligning IT portfolio processes with corporate objectives
- ☐ Selecting IT investment projects that align with corporate strategy
- ☐ Increasing the budget and resources allocated for IT investments
- ☐ Determining the opportunity cost of IT investment projects

Question 1696

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 1697

Which of the following would be the BEST population to take a sample from when testing program changes?

- ☐ Test library listings
- ☐ Source program listings
- ☐ Program change requests
- ☒ Production library listings

Explanation:

Explanation:

The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process

Licensed to Berend Post berend.post@it-university.nl

organizational data. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

Question 1698

Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

- ☐ Bridge
- ☐ Repeater
- ☐ Router
- ☒ Gateway

Explanation:

Explanation:

A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

Important Note:

For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.

The second thing you must remembers is the fact that a gateway act as a translation device.

It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.

For your exam you should know the information below:

Repeaters

A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

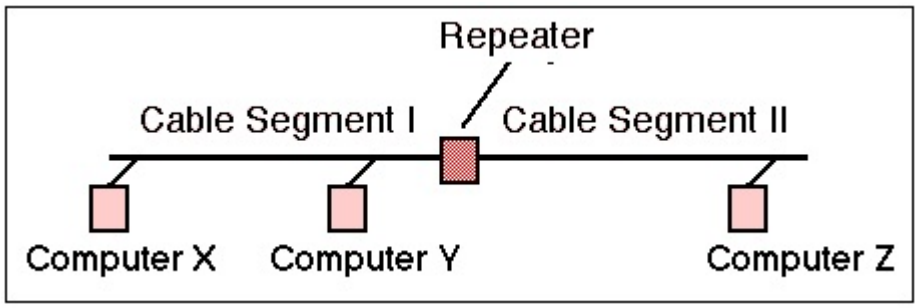
Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier.

Licensed to Berend Post berend.post@it-university.nl

If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.

A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

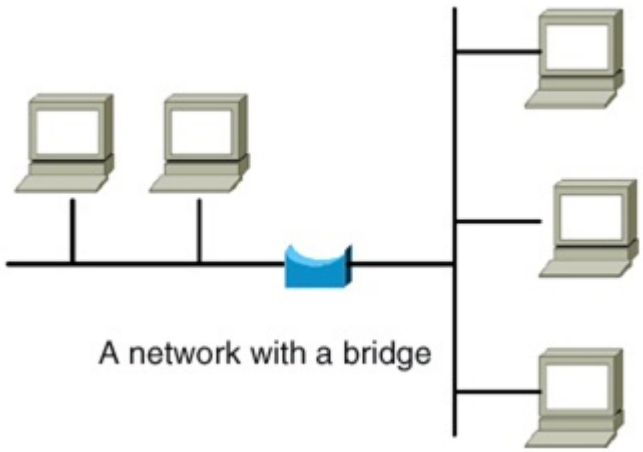
Repeater



Bridges

A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

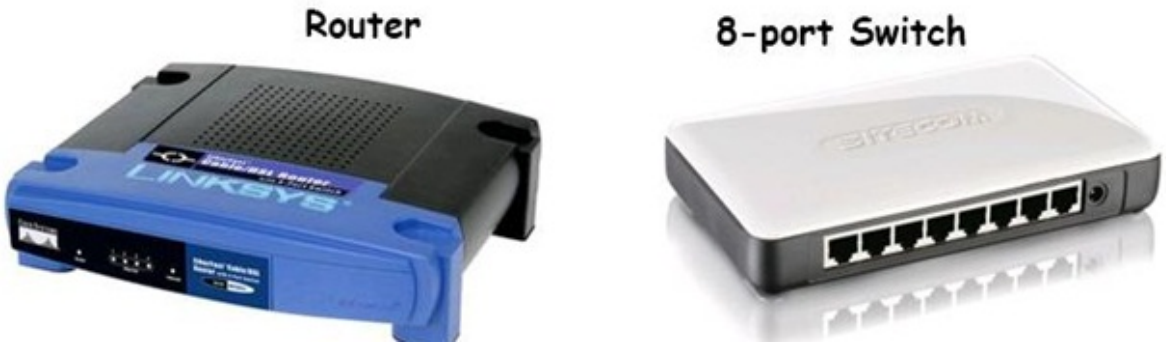


Licensed to Berend Post berend.post@it-university.nl

Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch



Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

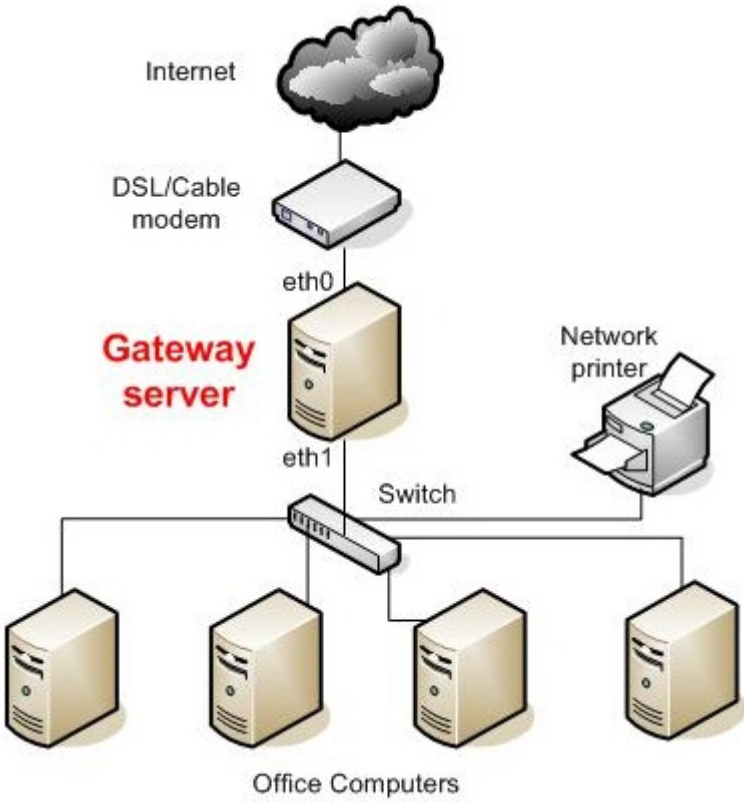
Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol

packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

Licensed to Berend Post berend.post@it-university.nl



The following answers are incorrect:

Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.

Reference:

CISA review manual 2014 Page number 263

Licensed to Berend Post berend.post@it-university.nl

Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

Question 1699

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

- ☐ evaluate the record retention plans for off-premises storage.
- ☒ interview programmers about the procedures currently being followed.
- ☐ compare utilization records to operations schedules.
- ☐ review data file access records to test the librarian function.

Explanation:

Explanation:

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the

access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

Question 1700

Which of the following is the PRIMARY advantage of the IT portfolio management approach over the balanced scorecard approach when managing IT investments?

- ☐ The influence of qualitative factors on investment decisions.
- ☐ Agility in adjusting investment decisions.
- ☐ Incorporation of organizational strategy in investment decisions.
- ☒ Use of the organization's risk appetite in investment decisions.

Question 1701

Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

- ☐ Field checks
- ☐ Control totals
- ☐ Reasonableness checks
- ☒ A before-and-after maintenance report

Explanation:

Explanation:

A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

Licensed to Berend Post berend.post@it-university.nl

Question 1702

The BEST way to assure an organization's board of directors that IT strategies support business objectives is to:

- ☐ provide regular assessments of emerging technologies
- ☒ identify and report on the achievement of critical success factors (CSFs)
- ☐ confirm that IT strategies have been fully documented and disseminated
- ☐ ensure that senior business managers review IT budgets

Question 1703

An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- ☐ Electromagnetic interference (EMI)
- ☐ Cross-talk
- ☐ Dispersion
- ☒ Attenuation

Explanation:

Explanation:

Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMI) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

Question 1704

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:

Explanation:

In a hierarchical model, data is organized into a tree-like structure, implying a single parent for each record. A sort field keeps sibling records in a particular order.

For your exam you should know below information about database models:

Licensed to Berend Post berend.post@it-university.nl

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

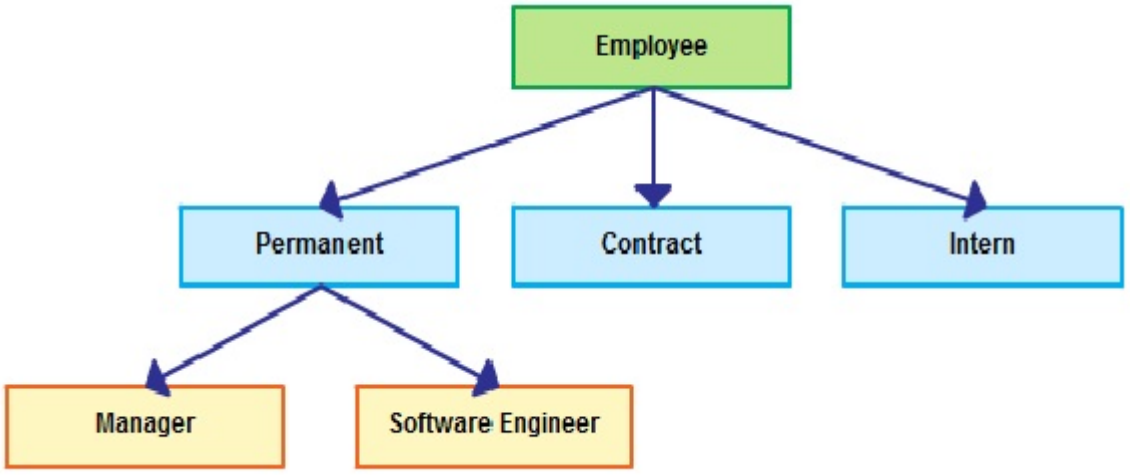
Hierarchical database model

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.

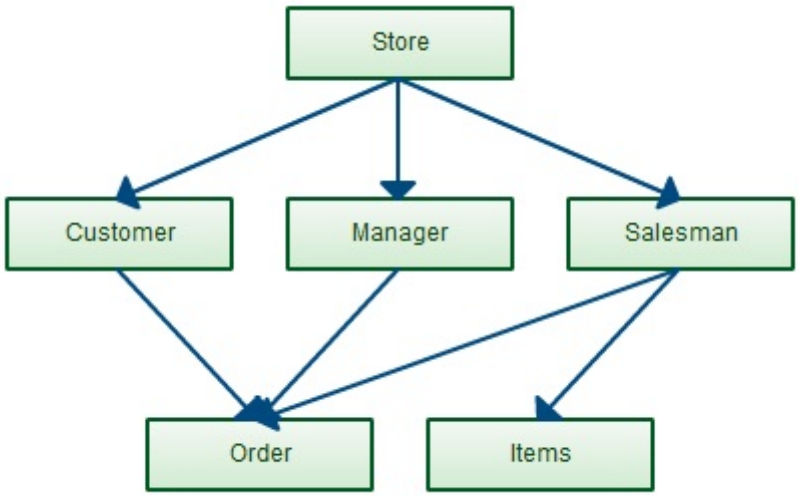
The network model organizes data using two fundamental concepts, called records and sets. Records contain fields (which may be organized hierarchically, as in the programming language COBOL). Sets (not to be confused with mathematical sets) define one-to-many[disambiguation needed] relationships between 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.

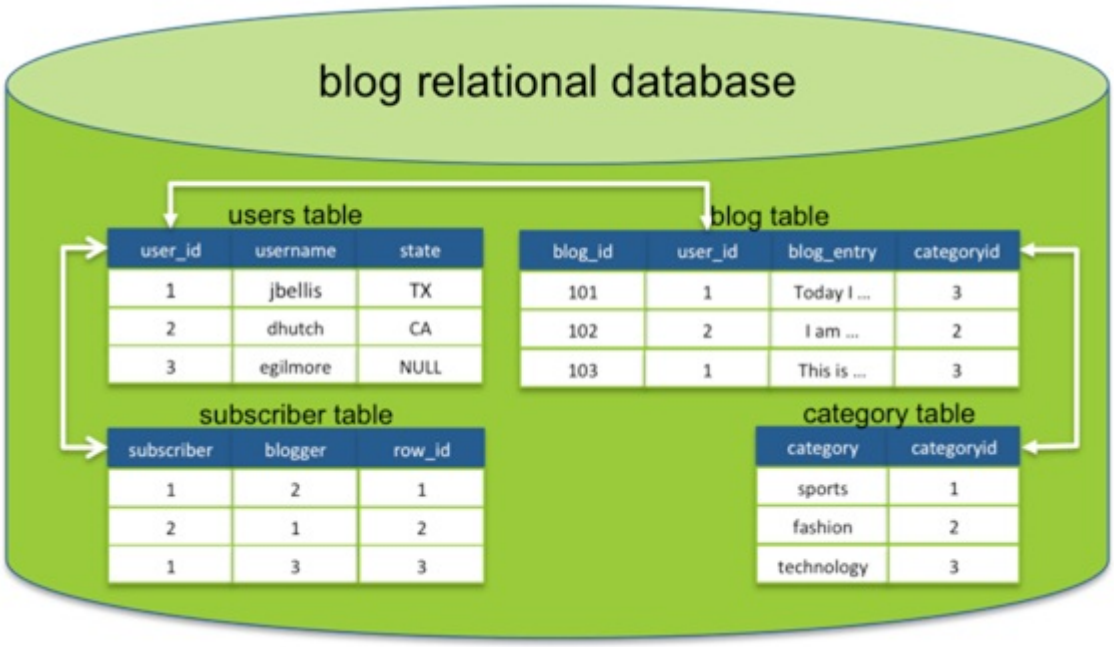
In the relational model, related records are linked together with a "key".

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.

Reference:

CISA review manual 2014 Page number 254

Question 1705

When physical destruction is not practical, which of the following is the MOST effective means of disposing of sensitive data on a hard disk?

- ☐ Recycling the disk
- ☐ Reformatting
- ☐ Deleting files sequentially
- ☒ Overwriting multiple times

Question 1706

Which of the following is a mechanism for mitigating risks?

- ☒ Security and control practices
- ☐ Property and liability insurance
- ☐ Audit and certification
- ☐ Contracts and service level agreements (SLAs)

Explanation:

Explanation:

Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, while contracts and SLAs are mechanisms of risk allocation.

Question 1707

In an EDI process, the device which transmits and receives electronic documents is the:

- ☒ communications handler.
- ☐ EDI translator.
- ☐ application interface.
- ☐ EDI interface.

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

Question 1708

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.

Question 1709

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 1710

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

Licensed to Berend Post berend.post@it-university.nl

Question 1711

The FIRST course of action an investigator should take when a computer is being attacked is to:

- ☐ terminate all active processes.
- ☐ copy the contents of the hard drive.
- ☒ disconnect it from the network.
- ☐ disconnect the power source.

Question 1712

As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

- ☐ Organizational risks, such as single point-of-failure and infrastructure risk
- ☐ Threats to critical business processes
- ☒ Critical business processes for ascertaining the priority for recovery
- ☐ Resources required for resumption of business

Explanation:

Explanation:

The identification of the priority for recovering critical business processes should be addressed first. Organizational risks should be identified next, followed by the identification of threats to critical business processes. Identification of resources for business resumption will occur after the tasks mentioned.

Question 1713

An IS auditor notes that several of a client's servers are vulnerable to attack due to open unused ports and protocols. The auditor recommends management implement minimum security requirements. Which type of control has been recommended?

- ☒ Preventive
- ☐ Corrective
- ☐ Directive
- ☐ Compensating

Question 1714

During the evaluation of a firm's newly established whistleblower system, an auditor notes several findings. Which of the following should be the auditor's GREATEST concern?

- ☐ New employees have not been informed of the whistleblower policy.
- ☒ The whistleblower's privacy is not protected.
- ☐ The whistleblower system does not track the time and date of submission.
- ☐ The whistleblower system is only available during business hours.

Licensed to Berend Post berend.post@it-university.nl

Question 1715

In-house personnel performing IS audits should possess which of the following knowledge and/or skills (Choose two.):

- ☒ information systems knowledge commensurate with the scope of the IT environment in question
- ☒ sufficient analytical skills to determine root cause of deficiencies in question
- ☐ sufficient knowledge on secure system coding
- ☐ sufficient knowledge on secure platform development
- ☐ information systems knowledge commensurate outside of the scope of the IT environment in question

Explanation:

Explanation:

Personnel performing IT audits should have information systems knowledge commensurate with the scope of the institution's IT environment. They should also possess sufficient analytical skills to determine the root cause of deficiencies.

Question 1716

Following a breach, what is the BEST source to determine the maximum amount of time before customers must be notified that their personal information may have been compromised?

- ☐ Industry standards
- ☐ Information security policy
- ☐ Incident response plan
- ☒ Industry regulations

Question 1717

An IS steering committee should:

- ☐ include a mix of members from different departments and staff levels.
- ☐ ensure that IS security policies and procedures have been executed properly.
- ☒ have formal terms of reference and maintain minutes of its meetings.
- ☐ be briefed about new trends and products at each meeting by a vendor.

Explanation:

Explanation:

It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

Licensed to Berend Post berend.post@it-university.nl

Question 1718

In a typical SDLC, which group is PRIMARILY responsible for confirming compliance with requirements?

- ☐ Steering committee
- ☐ Risk management
- ☒ Quality assurance
- ☐ Internal audit

Question 1719

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.

Question 1720

When conducting a requirements analysis for a project the BEST approach would be to:

- ☐ conduct a control self-assessment.
- ☒ consult key stakeholders.
- ☐ test operational deliverables.
- ☐ prototype the requirements.

Question 1721

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:

Licensed to Berend Post berend.post@it-university.nl

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 1722

Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

- ☐ Acceptance testing is to be managed by users.
- ☒ A quality plan is not part of the contracted deliverables.
- ☐ Not all business functions will be available on initial implementation.
- ☐ Prototyping is being used to confirm that the system meets business requirements.

Explanation:

Explanation:

A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

Question 1723

Which of the following attacks could capture network user passwords?

- ☐ Data diddling
- ☒ Sniffing
- ☐ IP Spoofing
- ☐ Surfing

Explanation:

Explanation:

A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.

Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A

Licensed to Berend Post berend.post@it-university.nl

hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap—a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therefore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:

Data did dlinginvolves changing data before, as it is entered into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Surfing would refer to the surf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

Reference:

CISA Review manual 2014 Page number 321

Official ISC2 Guide to the CISSP 3rd edition Page Number 153

Licensed to Berend Post berend.post@it-university.nl

Question 1724

An organization using instant messaging to communicate with customers can prevent legitimate customers from being impersonated by:

- ☐ using call monitoring.
- ☐ using firewalls to limit network traffic to authorized ports.
- ☐ logging conversations.
- ☒ authenticating users before conversations are initiated.

Question 1725

The purpose of a deadman door controlling access to a computer facility is primarily to:

- ☒ prevent piggybacking.
- ☐ prevent toxic gases from entering the data center.
- ☐ starve a fire of oxygen.
- ☐ prevent an excessively rapid entry to, or exit from, the facility.

Explanation:

Explanation:

The purpose of a deadman door controlling access to a computer facility is primarily intended to prevent piggybacking. Choices B and C could be accomplished with a single self-closing door. Choice D is invalid, as a rapid exit may be necessary in some circumstances, e.g., a fire.

Question 1726

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 1727

To enable the alignment of IT staff development plans with IT strategy, which of the following should be done FIRST?

- ☒ Include strategic objectives in IT staff performance objectives.
- ☐ Review IT staff job descriptions for alignment.
- ☐ Identify required IT skill sets that support key business processes.
- ☐ Develop quarterly training for each IT staff member.

Licensed to Berend Post berend.post@it-university.nl

Question 1728

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 1729

In an organization that has a staff-rotation policy, the MOST appropriate access control model is:

- ☒ role based.
- ☐ discretionary.
- ☐ mandatory.
- ☐ lattice based.

Question 1730

To determine who has been given permission to use a particular system resource, an IS auditor should review:

- ☐ activity lists.
- ☒ access control lists.
- ☐ logon ID lists.
- ☐ password lists.

Explanation:

Explanation:

Access control lists are the authorization tables that document the users who have been given permission to use a particular system resource and the types of access they have been granted. The other choices would not document who has been given permission to use (access) specific system resources.

Licensed to Berend Post berend.post@it-university.nl

Question 1731

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.

Question 1732

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 1733

An IS auditor finds that conference rooms have active network ports. Which of the following is MOST important to ensure?

- ☐ The corporate network is using an intrusion prevention system (IPS)
- ☒ This part of the network is isolated from the corporate network
- ☐ A single sign-on has been implemented in the corporate network
- ☐ Antivirus software is in place to protect the corporate network

Explanation:

Explanation:

If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or being physically separated. An I PS would detect possible attacks, but only after they have

Licensed to Berend Post berend.post@it-university.nl

occurred. A single sign-on would ease authentication management. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

Question 1734

What can be used to help identify and investigate unauthorized transactions?

- ☐ Postmortem review
- ☐ Reasonableness checks
- ☒ Data-mining techniques
- ☐ Expert systems

Explanation:

Explanation:

Data-mining techniques can be used to help identify and investigate unauthorized transactions.

Question 1735

Which of the following is the MOST important security consideration when using infrastructure as a Service (IaaS)?

- ☒ User access management
- ☐ Compliance with internal standards
- ☐ Segmentation among guests
- ☐ Backup and recovery strategy

Question 1736

Which of the following has the GREATEST influence on the success of IT governance?

- ☐ IT strategy is embedded in all risk management processes
- ☒ Alignment of IT strategies with the entity's vision
- ☐ The CIO is a member of the audit committee
- ☐ Clear, concise, and enforced IS policies

Question 1737

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

- ☒ True
- ☐ False

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

Question 1738

Most trojan horse programs are spread through:

- ☒ e-mails.
- ☐ MP3.
- ☐ MS Office.
- ☐ Word template.
- ☐ None of the choices.

Explanation:

Explanation:

"Most trojan horse programs are spread through e-mails. Some earlier trojan horse programs were bundled in "Root Kits". For example, the Linux Root Kit version 3 (lrk3) which was released in December 96 had tcp wrapper trojans included and enhanced in the kit. Portable devices that run Linux can also be affected by trojan horse. The Trojan.Linux.JBellz Trojan horse runs as a malformed .mp3 file."

Question 1739

In a complex IS environment, which of the following tasks should be performed by the data owner?

- ☐ Perform technical database maintenance.
- ☐ Perform data restoration when necessary.
- ☒ Review data classifications periodically.
- ☐ Test the validity of backup data.

Question 1740

Which of the following external entities would provide the BEST guidance to an organization facing advanced attacks?

- ☒ Recognized threat intelligence communities
- ☐ Open-source reconnaissance
- ☐ Disaster recovery consultants widely endorsed in industry forums
- ☐ Incident response experts from highly regarded peer organizations

Licensed to Berend Post berend.post@it-university.nl

Question 1741

Which of the following functionality is NOT supported by SSL protocol?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Authentication
- ☒ Availability

Explanation:

Explanation:

The NOT is a keyword used in this question. You need to find out the functionality which is NOT provided by SSL protocol. The SSL protocol provides:

Confidentiality

Integrity

Authentication, e.g. between client and server

Non-repudiation

For CISA exam you should know the information below about Secure Socket Layer (SSL) and Transport Layer Security (TLS)

These are cryptographic protocols which provide secure communication on Internet. There are only slight difference between SSL 3.0 and TLS 1.0. For general concept both are called SSL.

SSL is session-connection layer protocol widely used on Internet for communication between browser and web servers, where any amount of data is securely transmitted while a session is established. SSL provides end point authentication and communication privacy over the Internet using cryptography. In typical use, only the server is authenticated while client remains unauthenticated. Mutual authentication requires PKI development to clients. The protocol allows application to communicate in a way designed to prevent eavesdropping, tampering and message forging.

SSL involves a number of basic phases

Peer negotiation for algorithm support

Public-key, encryption based key exchange and certificate based authentication

Symmetric cipher based traffic encryption.

Licensed to Berend Post berend.post@it-university.nl

SSL runs on a layer beneath application protocol such as HTTP, SMTP and Network News Transport Protocol (NNTP) and above the TCP transport protocol, which forms part of TCP/IP suite.

SSL uses a hybrid hashed, private and public key cryptographic processes to secure transmission over the INTERNET through a PKI.

The SSL handshake protocol is based on the application layer but provides for the security of the communication session too. It negotiates the security parameter for each communication section. Multiple session can belong to one SSL session and the participating in one session can take part in multiple simultaneous sessions.

The following were incorrect answers:

Confidentiality - It is supported by the SSL Protocol

Integrity -It is supported by the SSL Protocol

Authentication - It is supported by the SSL protocol

Reference:

CISA review manual 2014 Page number 352

Question 1742

Which of the following would BEST deter the theft of corporate information from a laptop?

- ☐ Install biometric access controls.
- ☒ Encrypt all data on the hard drive.
- ☐ Protect files with passwords.
- ☐ Encrypt the file allocation table (FAT).

Question 1743

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:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

Most encrypted transactions use a combination of private keys, public keys, secret keys, hash functions and digital certificates to achieve confidentiality, message integrity and nonrepudiation by either sender or recipient. The recipient uses the sender's public key to decrypt the prehash code into a posthash code, which when equaling the prehash code, verifies the identity of the sender and that the message has not been changed in route; this would provide the greatest assurance. Each sender and recipient has a private key known only to themselves and a public key, which can be known by anyone. Each encryption/decryption process requires at least one public key and one private key, and both must be from the same party. A single, secret key is used to encrypt the message, because secret key encryption requires less processing power than using public and private keys. A digital certificate, signed by a certificate authority, validates senders' and recipients' public keys.

Question 1744

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

- ☐ Mobile
- ☒ Redundant
- ☐ Shared
- ☐ Warm

Question 1745

What is an edit check to determine whether a field contains valid data?

- ☒ Completeness check
- ☐ Accuracy check
- ☐ Redundancy check
- ☐ Reasonableness check

Explanation:

Explanation:

A completeness check is an edit check to determine whether a field contains valid data.

Licensed to Berend Post berend.post@it-university.nl

Question 1746

An IS auditor concludes that a local area network's (LAN's) access security is satisfactory. In reviewing the work, the audit manager should:

- ☐ re-perform some steps of the audit to verify the quality of the work.
- ☒ verify that the elements of an agreed-upon audit plan have been addressed.
- ☐ verify user management's agreement with the findings.
- ☐ assess whether the auditor had the appropriate skills to perform the work.

Question 1747

The PRIMARY purpose for an IS auditor to review previous audit reports during the planning phase of a current audit is to:

- ☐ become informed about the auditee's business processes.
- ☐ adjust audit scope to reduce testing in areas related to previous findings.
- ☐ identify applicable regulatory requirements for the current audit.
- ☒ ensure that previously identified risks are addressed in the audit program.

Question 1748

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

- ☐ test data covering critical applications.
- ☐ detailed test plans.
- ☐ quality assurance test specifications.
- ☒ user acceptance testing specifications

Explanation:

Explanation: A key objective in any software development project is to ensure that the developed software will meet the business objectives and the requirements of the user. The users should be involved in the requirements definition phase of a development project and user acceptance test specification should be developed during this phase. The other choices are generally performed during the system testing phase.

Question 1749

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

- ☐ Embedded audit module
- ☐ Integrated test facility
- ☐ Snapshots
- ☒ Audit hooks

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Explanation:

The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially-written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audit trail is required.

Question 1750

Which of the following is MOST important to include in a business continuity plan (BCP)?

- ☐ Vendor contact information
- ☒ Documentation of critical systems
- ☐ Documentation of data center floor plans
- ☐ Backup site location information

Question 1751

When developing metrics to measure the contribution of IT to the achievement of business goals, the MOST important consideration is that the metrics:

- ☐ measure the effectiveness of IT controls in the achievement of IT strategy.
- ☐ provide quantitative measurement of IT initiatives in relation with business targets.
- ☒ are expressed in terms of how IT risk impacts the achievement of business goals.
- ☐ are used by similar industries to measure the effect of IT on business strategy.

Question 1752

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1753

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- ☐ test data to validate data input.
- ☐ test data to determine system sort capabilities.
- ☒ generalized audit software to search for address field duplications.
- ☐ generalized audit software to search for account field duplications.

Explanation:

Explanation:

Since the name is not the same {due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

Question 1754

Effective transactional controls are often capable of offering which of the following benefits (Choose four.):

- ☒ reduced administrative and material costs
- ☒ shortened contract cycle times
- ☒ enhanced procurement decisions
- ☒ diminished legal risk
- ☐ None of the choices.

Explanation:

Explanation:

Transactional systems provide a baseline necessary to measure and monitor contract performance and provide a method for appraising efficiency against possible areas of exposure. Effective transactional controls reduce administrative and material costs, shorten contract cycle times, enhance procurement decisions, and diminish legal risk.

Licensed to Berend Post berend.post@it-university.nl

Question 1755

After observing suspicious activities in a server, a manager requests a forensic analysis.
Which of the following findings should be of MOST concern to the investigator?

- ☐ Server is a member of a workgroup and not part of the server domain
- ☐ Guest account is enabled on the server
- ☐ Recently, 100 users were created in the server
- ☒ Audit logs are not enabled for the server

Explanation:

Explanation:

Audit logs can provide evidence which is required to proceed with an investigation and should not be disabled. For business needs, a server can be a member of a workgroup and, therefore, not a concern. Having a guest account enabled on a system is a poor security practice but not a forensic investigation concern. Recently creating 100 users in the server may have been required to meet business needs and should not be a concern.

Question 1756

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

- ☐ Specific developments only
- ☐ Business requirements only
- ☒ All phases of the installation must be documented
- ☐ No need to develop a customer specific documentation

Explanation:

Explanation:

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

Licensed to Berend Post berend.post@it-university.nl

Question 1757

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:

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

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

Licensed to Berend Post berend.post@it-university.nl

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

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

Licensed to Berend Post berend.post@it-university.nl

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

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

Licensed to Berend Post berend.post@it-university.nl

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:

The other options presented correctly describes PBX features thus not the right choice.

Reference:

CISA review manual 2014 Page number358

Question 1758

The scheduling of audit follow-ups should be based PRIMARILY on:

- ☐ costs and audit efforts involved.
- ☐ auditee and auditor time commitments.
- ☒ the risk and exposure involved.
- ☐ control and detection processes.

Licensed to Berend Post berend.post@it-university.nl

Question 1759

Due to the increasing size of a database, user access times and daily backups continue to increase. Which of the following would be the BEST way to address this situation?

- ☐ Data modeling
- ☐ Data visualization
- ☐ Data mining
- ☒ Data purging

Question 1760

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 1761

Which of the following is the PRIMARY benefit of implementing configuration management for IT?

- ☐ It helps audit in verifying IT conformance to business requirements.
- ☐ It establishes the dependency of application systems with various IT assets.
- ☐ It provides visibility to the overall function and technical attributes of IT assets.
- ☒ It helps automate change and release management processes in IT.

Question 1762

During a review of the IT strategic plan, an IS auditor finds several IT initiatives focused on delivering new systems and technology are not aligned with the organization's strategy. Witch of the following would be the IS auditor's BEST recommendation?

- ☐ Reassess the return on investment for the IT initiatives
- ☐ Modify IT initiatives that do not map to business strategies
- ☐ Utilize a balanced scorecard to align IT initiatives to business strategies
- ☒ Reassess IT initiatives that do not map business strategies

Licensed to Berend Post berend.post@it-university.nl

Question 1763

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 1764

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 1765

An organization wants to classify database tables according to its data classification scheme. From an IS auditor's perspective, the tables should be classified based on the:

- ☐ number of end users with access to the table
- ☐ frequency of updates to the table
- ☐ descriptions of column names in the table
- ☒ specific functional contents of each single table

Question 1766

Which of the following metrics would be MOST helpful to an IS auditor in evaluating an organization's security incident response management capability?

- ☒ Number of business interruptions due to IT security incidents per year.
- ☐ Number of IT security incidents reported per month
- ☐ Number of malware infections in business applications detected per day.
- ☐ Number of alerts generated by intrusion detection systems (IDS) per minute.

Licensed to Berend Post berend.post@it-university.nl

Question 1767

Which of the following is the PRIMARY advantage of having an established information security governance framework in place when an organization is adopting emerging technologies?

- ☐ An emerging technologies strategy would be in place
- ☐ A cost-benefit analysis process would be easier to perform
- ☒ An effective security risk management process is established
- ☐ End-user acceptance of emerging technologies has been established

Question 1768

Which of the following would be MOST useful when analyzing computer performance?

- ☐ Report of off-peak utilization and response time
- ☒ Tuning of system software to optimize resource usage
- ☐ Operations report of user dissatisfaction with response time
- ☐ Statistical metrics measuring capacity utilization

Question 1769

Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

- ☐ Application layer – Telnet
- ☒ Transport layer – ICMP
- ☐ Internet layer – IP
- ☐ Network Access layer – Ethernet

Explanation:

Explanation:

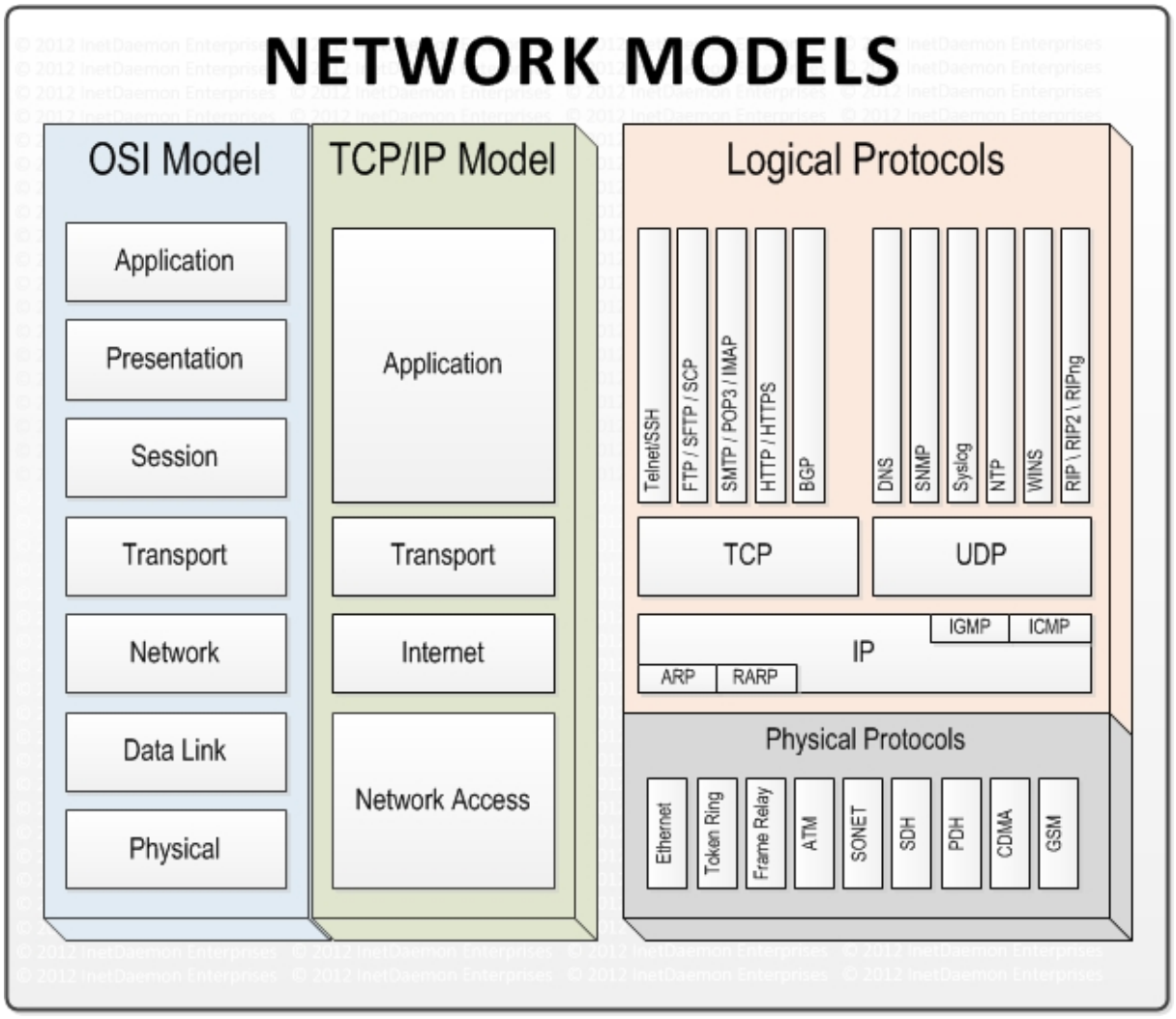
The keyword INCORRECT is used within the question. You need to find out the incorrect Layer to Protocol mapping.

The ICMP protocol works at Internet layer of the DoD TCP/IP model, not at the Transport Layer.

For your exam you should know below information about the TCP/IP models:

Network Models

Licensed to Berend Post berend.post@it-university.nl



Layer 4. Application Layer

Application layer is the top most layer of four layer TCP/IP model. Application layer is present on the top of the Transport layer. Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.

Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol) , DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Layer 3. Transport Layer

Transport Layer is the third layer of the four layer TCP/IP model. The position of the Transport layer is between Application layer and Internet layer. The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation. Transport layer defines the level of service and status of the connection used when transporting data.

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.

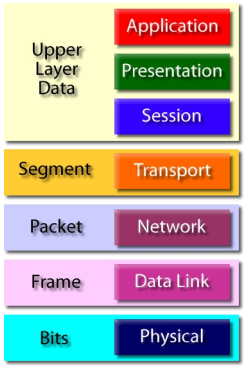
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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):



The following answers are incorrect:

The other options correctly describe the Layer to Protocol mapping of the DoD TCP/IP model protocols.

Reference:

CISA review manual 2014 page number 272

Question 1770

Which of the following is the BEST time for an IS auditor to perform a post-implementation review?

- ☒ When the system has stabilized.
- ☐ After the completion of user testing.
- ☐ Before decommissioning the legacy system.
- ☐ Immediately after the new system goes into production.

Licensed to Berend Post berend.post@it-university.nl

Question 1771

One advantage of monetary unit sampling is the fact that:

- ☒ results are stated in terms of the frequency of items in error
- ☐ it can easily be applied manually when computer resources are not available
- ☐ it increases the likelihood of selecting material items from the population
- ☐ large-value population items are segregated and audited separately

Question 1772

Which of the following procedures should an IS auditor complete FIRST when evaluating the adequacy of IT key performance indicators (KPIs)?

- ☐ Independently calculate the accuracy of the KPIs.
- ☐ Review KPIs that indicate poor IT performance.
- ☐ Validate the KPI thresholds.
- ☒ Determine whether the KPIs support IT objectives.

Question 1773

A database administrator should be prevented from:

- ☐ using an emergency user ID.
- ☒ accessing sensitive information.
- ☐ having end user responsibilities.
- ☐ having access to production files.

Question 1774

The MAIN reason an organization's incident management procedures should include a post-incident review is to:

- ☐ ensure evidence is collected for possible post-event litigation.
- ☐ take appropriate action when procedures are not followed.
- ☐ enable better reporting for executives and the audit committee.
- ☒ improve processes by learning from identified weaknesses.

Question 1775

An IS auditor's role in privacy and security is to:

- ☐ assist in developing an IS security strategy.
- ☐ verify compliance with applicable laws.
- ☐ implement risk management methodologies.
- ☒ assist the governance steering committee with implementing a security policy.

Licensed to Berend Post berend.post@it-university.nl

Question 1776

When conducting a post-implementation review, which of the following is the BEST way to determine whether the value from an IT project has been achieved?

- ☐ Calculate the return on investment (ROI).
- ☐ Interview stakeholders.
- ☒ Conduct an earned value analysis (EVA).
- ☐ Survey end users.

Question 1777

Which of the following is the MOST important privacy consideration for an organization that uses a cloud service provider to process customer data?

- ☐ Data privacy must be monitored in accordance with industry standards and best practices.
- ☐ All customer data transferred to the service provider must be reported to the regulatory authority.
- ☐ No personal information may be transferred to the service provider without the consent of the customer.
- ☒ Data privacy must be managed in accordance with the regulations applicable to the organization.

Question 1778

The PRIMARY objective of business continuity and disaster recovery plans should be to:

- ☐ safeguard critical IS assets.
- ☐ provide for continuity of operations.
- ☐ minimize the loss to an organization.
- ☒ protect human life.

Explanation:

Explanation:

Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

Licensed to Berend Post berend.post@it-university.nl

Question 1779

Which of the following findings should be of GREATEST concern to an IS auditor performing a review of IT operations?

- ☐ The job scheduler application has not been designed to display pop-up error messages.
- ☐ Access to the job scheduler application has not been restricted to a maximum of two staff members.
- ☒ Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor.
- ☐ Operations shift turnover logs are not utilized to coordinate and control the processing environment.

Question 1780

Which of the following is the BEST evidence that an organization is aware of applicable laws and regulations?

- ☒ The organization's compliance matrix
- ☐ History of legal actions and regulatory correspondence
- ☐ The existence of an employee awareness training program
- ☐ Industry benchmark results

Question 1781

Which of the following is a good tool to use to help enforcing the deployment of good passwords?

- ☒ password cracker
- ☐ local DoS attacker
- ☐ network hacker
- ☐ remote windowing tool
- ☐ None of the choices.

Explanation:

Explanation:

"Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters. You may want to run a "password cracker" program periodically, and require users to immediately change any easily cracked passwords. In any case ask them to change their passwords every 90 to 120 days."

Licensed to Berend Post berend.post@it-university.nl

Question 1782

Which of the following provides the BEST evidence of successfully completed batch uploads?

- ☐ Sign-off on the batch journal
- ☐ Using sequence controls
- ☐ Enforcing batch cut-off times
- ☒ Reviewing process logs

Question 1783

Which of the following is the PRIMARY concern if a business continuity plan (BCP) is not based on a business impact analysis (BIA)?

- ☐ The critical systems were not identified, but all systems are covered in the BCP.
- ☐ The knowledge of key people within the organization was not considered in the BCP.
- ☐ The strategy of the BCP does not reflect estimated potential losses.
- ☒ Management was not involved in the early stages of the BCP.

Question 1784

As part of business continuity planning, which of the following is MOST important to include in a business impact analysis (BIA)?

- ☐ Define a risk appetite.
- ☐ Assess risk of moving significant applications to the cloud.
- ☐ Assess recovery scenarios.
- ☒ Assess threats to the organization.

Question 1785

Which of the following risks could result from inadequate software baselining?

- ☒ Scope creep
- ☐ Sign-off delays
- ☐ Software integrity violations
- ☐ inadequate controls

Explanation:

Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. Choices, C and D may not always result, but choice A is inevitable.

Licensed to Berend Post berend.post@it-university.nl

Question 1786

In what way is a common gateway interface (CGI) MOST often used on a webserver?

- ☒ Consistent way for transferring data to the application program and back to the user
- ☐ Computer graphics imaging method for movies and TV
- ☐ Graphic user interface for web design
- ☐ interface to access the private gateway domain

Explanation:

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orienteering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

Question 1787

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 1788

What is the PRIMARY advantage of prototyping as part of systems development?

- ☒ Maximizes user satisfaction
- ☐ Eliminates the need for internal controls
- ☐ Increases accuracy in reporting
- ☐ Reduces the need for compliance testing

Licensed to Berend Post berend.post@it-university.nl

Question 1789

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 1790

If a database is restored using before-image dumps, where should the process begin following an interruption?

- ☒ Before the last transaction
- ☐ After the last transaction
- ☐ As the first transaction after the latest checkpoint
- ☐ At the last transaction before the latest checkpoint

Explanation:

Explanation:

If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

Question 1791

The Federal Information Processing Standards (FIPS) were developed by:

- ☒ the United States Federal government
- ☐ ANSI
- ☐ ISO
- ☐ IEEE
- ☐ IANA
- ☐ None of the choices.

Explanation:

Explanation:

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal government for use by all nonmilitary government agencies and by

Licensed to Berend Post berend.post@it-university.nl

government contractors. Many FIPS standards are modified versions of standards used in the wider community.

Question 1792

In RFID technology which of the following risk could represent a threat to non-RFID networked or collocated systems, assets, and people?

- ☐ Business Process Risk
- ☐ Business Intelligence Risk
- ☐ Privacy Risk
- ☒ Externality Risk

Explanation:

Explanation:

RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person.

Externality risks are present for both the RF and enterprise subsystems of an RFID system.

The main externality risk for the RF subsystem is hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance.

The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage.

The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application. Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

For your exam you should know the information below:

Licensed to Berend Post berend.post@it-university.nl

Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). Others use a local power source such as a battery, or else have no battery but collect energy from the interrogating EM field, and then act as a passive transponder to emit microwaves or UHF radio waves (i.e., electromagnetic radiation at high frequencies). Battery powered tags may operate at hundreds of meters. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader, and may be embedded in the tracked object.

RFID tags are used in many industries. An RFID tag attached to an automobile during production can be used to track its progress through the assembly line. Pharmaceuticals can be tracked through warehouses. Livestock and pets may have tags injected, allowing positive identification of the animal.

RFID RISKS

RFID technology enables an organization to significantly change its business processes to:

Increase its efficiency, which results in lower costs, Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk.

For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics. This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments.

The risks are as follows:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Licensed to Berend Post berend.post@it-university.nl

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Externality Risk -RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users.

The following answers are incorrect:

Business Process Risk -Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.

Business Intelligence Risk- An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

Privacy Risk - Personal privacy rights or expectations may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended or understood. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.

Reference:

CISA review manual 2014 page number 248

Licensed to Berend Post berend.post@it-university.nl

Question 1793

Who is responsible for providing technical support for the hardware and software environment by developing, installing and operating the requested system?

- ☒ System Development Management
- ☐ Quality Assurance
- ☐ User Management
- ☐ Senior Management

Explanation:

Explanation:

System Development Management provides technical support for hardware and software environment by developing, installing and operating the requested system.

For the CISA exam you should know the information below about roles and responsibilities of groups/individuals that may be involved in the development process are summarized below:

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training. User management is concerned primarily with the following questions:

Are the required functions available in the software?

How reliable is the software?

How effective is the software?

Is the software easy to use?

How easy is to transfer or adapt old data from preexisting software to this environment?

Is it possible to add new functions?

Does it meet regulatory requirement?

Project Steering Committee – Provides overall directions and ensures appropriate representation of the major stakeholders in the project's outcome. The project steering committee is ultimately responsible for all deliverables, project costs and schedules. This committee should be compromised of senior representative from each business area that will be significantly impacted by the proposed new system or system modifications.

Licensed to Berend Post berend.post@it-university.nl

System Development Management – Provides technical support for hardware and software environment by developing, installing and operating the requested system.

Project Manager – Provides day-to-day management and leadership of the project, ensures that project activities remain in line with the overall directions, ensures appropriate representation of the affected departments, ensures that the project adheres local standards, ensures that deliverable meet the quality expectation of key stakeholder, resolve interdepartmental conflict, and monitors and controls cost of the project timetables.

Project Sponsor – Project sponsor provides funding for the project and works closely with the project manager to define critical success factor(CSFs) and metrics for measuring the success of the project. It is crucial that success is translated to measurable and quantifiable terms. Data and application ownership are assigned to a project sponsor. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

System Development Project Team – Completes assigned tasks, communicates effectively with user by actively involving them in the development process, works according to local standards, and advise the project manager of necessary plan deviations.

User Project Team – Completes assigned tasks, communicate effectively with the system developers by actively involving themselves in the development process as Subject Matter Expert (SME) and works according to local standards, and advise the project manager of expected and actual project deviations.

Security Officer – Ensures that system controls and supporting processes provides an effective level of protection, based on the data classification set in accordance with corporate security policies and procedures: consult throughout the life cycle on appropriate security measures that should be incorporated into the system.

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

The following were incorrect answers:

Quality Assurance – Personnel who review result and deliverables within each phase and at the end of each phase, and confirm compliance with requirements. Their objective is to ensure that the

 Licensed to Berend Post berend.post@it-university.nl

quality of the project by measuring adherence of the project staff to the organization's software development life cycle (SDLC), advise on the deviation and propose recommendation for process improvement or greater control points when deviation occur.

User Management – Assumes ownership of the project and resulting system, allocates qualified representatives to the team, and actively participates in business process redesign, system requirement definitions, test case development, acceptance testing and user training.

Senior Management – Demonstrate commitment to the project and approves the necessary resources to complete the project. This commitment from senior management helps ensure involvement by those needed to complete the project.

Reference:

CISA review manual 2014 Page number 150

Question 1794

The maturity level of an organization's problem management support function is optimized when the function:

- ☒ proactively provides solutions
- ☐ has formally documented the escalation process
- ☐ analyzes critical incidents to identify root cause
- ☐ resolves requests in a timely manner

Question 1795

Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

- ☐ Parallel Test
- ☐ Black box testing
- ☒ Regression Testing
- ☐ Pilot Testing

Explanation:

Explanation:

Regression testing is the process of rerunning a portion of a test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be same as original data.

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,

Licensed to Berend Post berend.post@it-university.nl

in a client server and web development, changes to the desktop environment. Multiple application may run on the user's desktop, potentially simultaneously, so it is important to test the impact of installing new dynamic link libraries (DLLs), making operating system registry or configuration file modification, and possibly extra memory utilization.

The following were incorrect answers:

Parallel Testing – This is the process of feeding test data into two systems – the modified system and an alternative system and comparing the result.

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

Reference:

CISA review manual 2014 Page number 167

Question 1796

There are many types of audit logs analysis tools available in the market. Which of the following audit logs analysis tools will look for anomalies in user or system behavior?

- ☐ Attack Signature detection tool
- ☒ Variance detection tool
- ☐ Audit Reduction tool
- ☐ Heuristic detection tool

Explanation:

Explanation:

Trend/Variance Detection tool are used to look for anomalies in user or system behavior. For example, if a user typically logs in at 9:00 am, but one day suddenly access the system at 4:30 am, this may indicate a security problem that may need to be investigated.

Licensed to Berend Post berend.post@it-university.nl

Other types of audit trail analysis tools should also be known for your CISA exam

The following were incorrect answers:

Audit Reduction tool - They are preprocessor designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tool can remove many audit records known to have little security significance.

Attack-signature detection tool - They look for an attack signature, which is a specific sequence of events indicative of an unauthorized access attempt. A simple example would be repeated failed logon attempts.

Heuristic detection tool - Heuristic analysis is an expert based analysis that determines the susceptibility of a system towards particular threat/risk using various decision rules or weighing methods. MultiCriteria analysis (MCA) is one of the means of weighing. This method differs with statistical analysis, which bases itself on the available data/statistics.

Reference:

CISA review manual 2014 Page number 336

and

http://en.wikipedia.org/wiki/Heuristic_analysis

Question 1797

The PRIMARY purpose of a precedence diagramming method in managing IT projects is to:

- ☐ monitor project scope creep.
- ☒ identify the critical path.
- ☐ identify key milestones.
- ☐ minimize delays and overruns.

Licensed to Berend Post berend.post@it-university.nl

Question 1798

Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

- ☐ RPO
- ☐ RTO
- ☒ WRT
- ☐ MTD

Explanation:

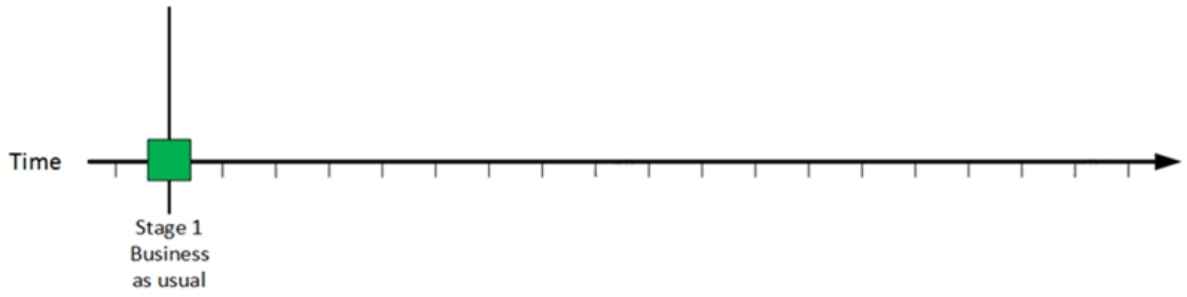
Explanation:

The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

For your exam you should know below information about RPO, RTO, WRT and MTD:

Stage 1: Business as usual

Business as usual

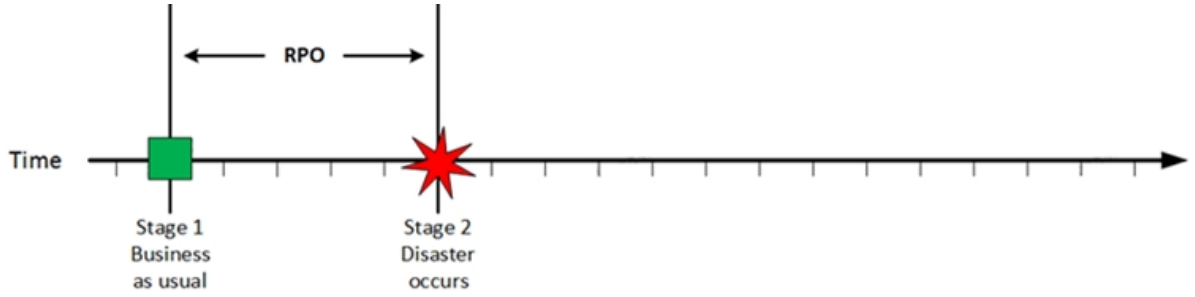


At this stage all systems are running production and working correctly.

Stage 2: Disaster occurs

Disaster Occurs

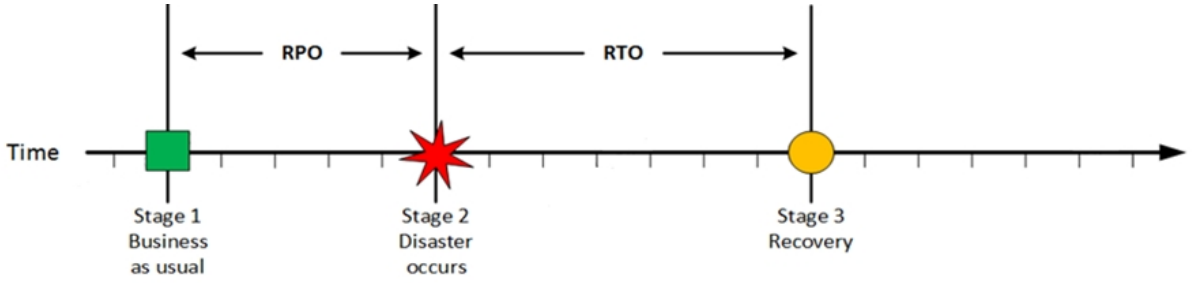
Licensed to Berend Post berend.post@it-university.nl



On a given point in time, disaster occurs and systems needs to be recovered. At this point the Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

Stage 3: Recovery

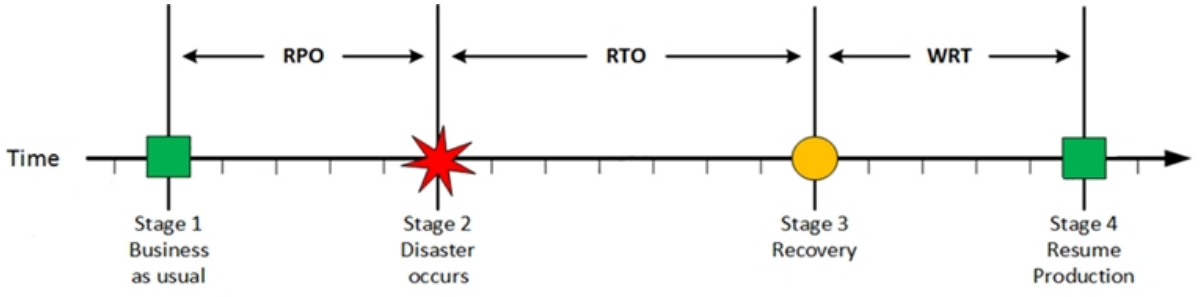
Recovery



At this stage the system are recovered and back online but not ready for production yet. The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

Stage 4: Resume Production

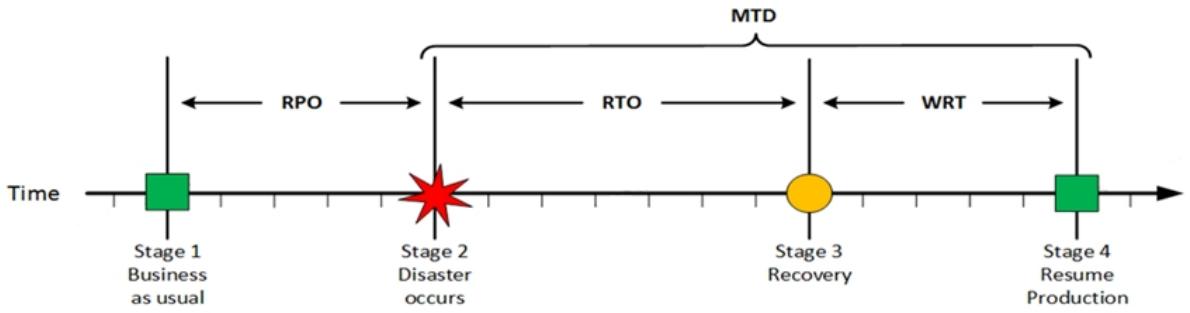
Resume Production



Licensed to Berend Post berend.post@it-university.nl

At this stage all systems are recovered, integrity of the system or data is verified and all critical systems can resume normal operations. The Work Recovery Time (WRT) determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity. This could be, for example, checking the databases and logs, making sure the applications or services are running and are available. In most cases those tasks are performed by application administrator, database administrator etc. When all systems affected by the disaster are verified and/or recovered, the environment is ready to resume the production again.

MTD



The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

The following answers are incorrect:

RPO - Recovery Point Objective (RPO) determines the maximum acceptable amount of data loss measured in time. For example, the maximum tolerable data loss is 15 minutes.

RTO - The Recovery Time Objective (RTO) determines the maximum tolerable amount of time needed to bring all critical systems back online. This covers, for example, restore data from back-up or fix of a failure. In most cases this part is carried out by system administrator, network administrator, storage administrator etc.

MTD - The sum of RTO and WRT is defined as the Maximum Tolerable Downtime (MTD) which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences. This value should be defined by the business management team or someone like CTO, CIO or IT manager.

Licensed to Berend Post berend.post@it-university.nl

Reference:

CISA review manual 2014 page number 284

http://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtdwth/

Question 1799

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 1800

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

- ☐ True
- ☒ False

Explanation:

Explanation:

An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

Licensed to Berend Post berend.post@it-university.nl

Question 1801

An IS auditor finds a number of system accounts that do not have documented approvals. Which of the following should be performed FIRST by the auditor?

- ☐ Have the accounts removed immediately
- ☐ Obtain sign-off on the accounts from the application owner
- ☐ Document a finding and report an ineffective account provisioning control
- ☒ Determine the purpose and risk of the accounts

Question 1802

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 1803

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:

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.

Licensed to Berend Post berend.post@it-university.nl

For your exam you should know the information below:

Common Types of computers

Supercomputers

A supercomputer is focused on performing tasks involving intense numerical calculations such as weather forecasting, fluid dynamics, nuclear simulations, theoretical astrophysics, and complex scientific computations. A supercomputer is a computer that is at the frontline of current processing capacity, particularly speed of calculation. The term supercomputer itself is rather fluid, and the speed of today's supercomputers tends to become typical of tomorrow's ordinary computer. Supercomputer processing speeds are measured in floating point operations per second, or FLOPS. An example of a floating point operation is the calculation of mathematical equations in real numbers. In terms of computational capability, memory size and speed, I/O technology, and topological issues such as bandwidth and latency, supercomputers are the most powerful, are very expensive, and not cost-effective just to perform batch or transaction processing. Transaction processing is handled by less powerful computers such as server computers or mainframes.

Mainframes

The term mainframe computer was created to distinguish the traditional, large, institutional computer intended to service multiple users from the smaller, single user machines. These computers are capable of handling and processing very large amounts of data quickly. Mainframe computers are used in large institutions such as government, banks and large corporations. They are measured in MIPS (million instructions per second) and respond to up to 100s of millions of users at a time.

Mid-range servers

Midrange systems are primarily high-end network servers and other types of servers that can handle the large-scale processing of many business applications. Although not as powerful as mainframe computers, they are less costly to buy, operate, and maintain than mainframe systems and thus meet the computing needs of many organizations. Midrange systems have become popular as powerful network servers to help manage large Internet Web sites, corporate intranets and extranets, and other networks. Today, midrange systems include servers used in industrial process-control and manufacturing plants and play major roles in computer-aided manufacturing (CAM). They can also take the form of powerful technical workstations for computer-aided design (CAD) and other computation and graphics-intensive applications. Midrange system are also used as front-end servers to assist mainframe computers in telecommunications processing and network management.

Personal computers

Licensed to Berend Post berend.post@it-university.nl

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.

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

Licensed to Berend Post berend.post@it-university.nl

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 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.

Reference:

CISA review manual 2014 page number 246

http://en.wikipedia.org/wiki/Thin_client

http://en.wikipedia.org/wiki/Mobile_device

http://en.wikipedia.org/wiki/Personal_computer

http://en.wikipedia.org/wiki/Classes_of_computers

http://en.wikipedia.org/wiki/Laptop

Licensed to Berend Post berend.post@it-university.nl

Question 1804

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 1805

You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?

- ☐ exploit
- ☒ vulnerability
- ☐ both

Explanation:

Explanation:

You should know the difference between an exploit and a vulnerability. An exploit refers to software, data, or commands capable of taking advantage of a bug, glitch or vulnerability in order to cause unintended behavior. Vulnerability in this sense refers to a weakness in the system.

Question 1806

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:

Licensed to Berend Post berend.post@it-university.nl

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.

Question 1807

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:

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:

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:

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 access layer - his layer operates to connect the data storage and quality layer with data stores in the data source layer and, in the process, avoiding the need to know to know exactly how these data stores are organized. Technology now permits SQL access to data even if it is not stored in a relational database.

Data preparation layer -This layer is concerned with the assembly and preparation of data for loading into data marts. The usual practice is to per-calculate the values that are loaded into OLAP data repositories to increase access speed.

Reference:

CISA review manual 2014 Page number 188

Question 1808

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 1809

Following an IS audit, which of the following types of risk would be MOST critical to communicate to key stakeholders?

- ☐ Control
- ☐ Residual
- ☒ Audit
- ☐ Inherent

Licensed to Berend Post berend.post@it-university.nl

Question 1810

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- ☐ Issue an audit finding
- ☐ Seek an explanation from IS management
- ☐ Review the classifications of data held on the server
- ☒ Expand the sample of logs reviewed

Explanation:

Explanation:

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

Question 1811

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:

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

Licensed to Berend Post berend.post@it-university.nl

channel to transact business. Companies can tailor their marketing strategies to an individual customer's needs and wants. As more of its business shifts on-line, a company will have an enhanced ability to track how its customer interact with it.

Business-to-Business (B-to-B) relationships – The relationship among the selling services of two or more business opens up the possibility of re-engineering business process across the boundaries that have traditionally separated external entities from each other. Because of the ease of access and the ubiquity of the Internet, for example companies can build business process that combine previously separated activities. The result is faster, higher quality and lower-cost set of transactions. The market has ever created to subdivision of B-to-B called business-to-small business(B-to-SB) relationships

Business-to-employee(B-to-E) relationships – Web technologies also assist in the dissemination of information to and among an organization employees.

Business-to-Government(B-to-G) relationships – covers all the transactions between companies and government organizations. Currently this category is infancy, but it could expand quit rapidly as government use their own operations to promote awareness and growth of e-commerce. In addition to public procurement, administrations may also offer the option of electronic interchange for such transactions as VAT returns and the payment of corporate taxes.

The following were incorrect answers:

The other options presented does not covers all transactions between companies and government organizations.

Reference:

CISA review manual 2014 Page number 175

Licensed to Berend Post berend.post@it-university.nl

Question 1812

An IS auditor notes that due to the small size of the organization, human resources staff can create new employees in the payroll system as well as process payroll. Which of the following is the BEST recommendation to address this situation?

- ☐ Outsource the processing of payroll to a third party.
- ☐ Implement a periodic user access review over the payroll system.
- ☐ Implement periodic reviews of employees in the payroll system.
- ☒ Hire additional staff so that access for the two functions can be segregated.

Question 1813

Which of the following IT service management activities is MOST likely to help with identifying the root cause of repeated instances of network latency?

- ☐ Incident management
- ☒ Problem management
- ☐ Change management
- ☐ Configuration management

Question 1814

Which of the following is MOST important for an IS auditor to consider when evaluating a Software as a Service (SaaS) arrangement?

- ☐ Total cost of ownership
- ☐ Frequency of software updates
- ☐ Physical security
- ☒ Software availability

Question 1815

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1816

Which of the following should be an IS auditor's PRIMARY focus when evaluating the response process for cyber crimes?

- ☐ Notification to regulators
- ☐ Communication with law enforcement
- ☒ Evidence collection
- ☐ Root cause analysis

Question 1817

Which of the following should be an IS auditor's PRIMARY consideration when evaluating the development and design of a privacy program?

- ☐ Data governance and data classification procedures
- ☐ Policies and procedures consistent with privacy guidelines
- ☒ Industry practice and regulatory compliance guidance
- ☐ Information security and incident management practices

Question 1818

Which of the following is the MOST important requirement for the successful implementation of security governance?

- ☐ Aligning to an international security framework
- ☒ Mapping to organizational strategies
- ☐ Implementing a security balanced scorecard
- ☐ Performing an enterprise-wide risk assessment

Question 1819

Following an acquisition, it was decided that legacy applications subject to compliance requirements will continue to be used until they can be phased out. The IS auditor needs to determine where there are control redundancies and where gaps may exist. Which of the following activities would be MOST helpful in making this determination?

- ☒ Control self-assessments
- ☐ Risk assessment
- ☐ Control testing
- ☐ Control mapping

Licensed to Berend Post berend.post@it-university.nl

Question 1820

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- ☒ Review and, where necessary, upgrade firewall capabilities
- ☐ Install modems to allow remote maintenance support access
- ☐ Create a physically distinct network to handle VoIP traffic
- ☐ Redirect all VoIP traffic to allow clear text logging of authentication credentials

Explanation:

Explanation:

Firewalls used as entry points to a Voice-over Internet Protocol (VoIP) network should be VoIP-capable. VoIP network services such as H.323 introduce complexities that are likely to strain the capabilities of older firewalls. Allowing for remote support access is an important consideration. However, a virtual private network (VPN) would offer a more secure means of enabling this access 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 1821

The GREATEST benefit in implementing an expert system is the:

- ☒ capturing of the knowledge and experience of individuals in an organization.
- ☐ sharing of knowledge in a central repository.
- ☐ enhancement of personnel productivity and performance.
- ☐ reduction of employee turnover in key departments.

Explanation:

Explanation:

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit; however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

Licensed to Berend Post berend.post@it-university.nl

Question 1822

A new information security manager is charged with reviewing and revising the information security strategy. The information security manager's FIRST course of action should be to gain an understanding of the organization's:

- ☐ security architecture
- ☐ risk register
- ☐ internal control framework
- ☒ business strategy

Question 1823

Which of the following is the BEST source of information for an IS auditor to use as a baseline to assess the adequacy of an organization's privacy policy?

- ☐ Benchmark studies of similar organizations
- ☒ Local privacy standards and regulations
- ☐ Historical privacy breaches and related root causes
- ☐ Globally accepted privacy best practices

Question 1824

Which of the following cloud deployment model operates solely for an organization?

- ☒ Private Cloud
- ☐ Community Cloud
- ☐ Public Cloud
- ☐ Hybrid Cloud

Explanation:

Explanation:

In Private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

For your exam you should know below information about Cloud Computing deployment models:

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

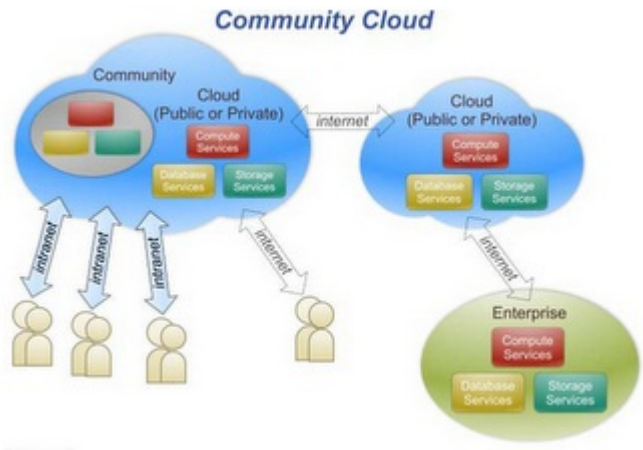
Private Cloud

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

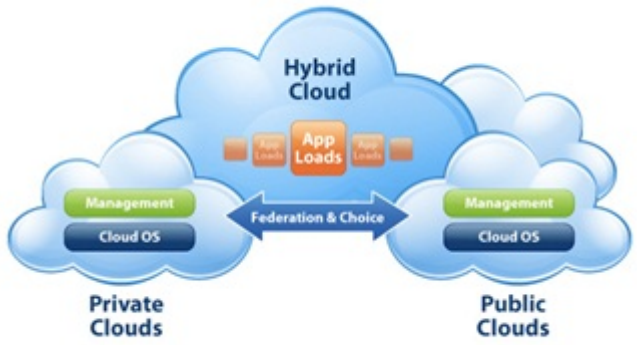


Public Cloud

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:

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Reference:

Licensed to Berend Post berend.post@it-university.nl

CISA review manual 2014 page number 102

Official ISC2 guide to CISSP 3rd edition Page number 689 and 690

Question 1825

The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will MOST likely:

- ☒ increase.
- ☐ decrease.
- ☐ remain the same.
- ☐ be unpredictable.

Explanation:

Explanation:

Due to the additional cost of disaster recovery planning (DRP) measures, the cost of normal operations for any organization will always increase after a DRP implementation, i.e., the cost of normal operations during a nondisaster period will be more than the cost of operations during a nondisaster period when no disaster recovery plan was in place.

Question 1826

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1827

During a review of an organization's IT incident management practices, the IS auditor finds the quality of incident resolution documentation is poor. Which of the following is the BEST recommendation to help address this issue?

- ☐ Have service desk staff create documentation be choosing from pre-selected answers in the service management tool.
- ☐ Require service desk staff to open incident tickets only when they have sufficient information.
- ☒ Revise incident resolution procedures and provide training for service desk staff on the applicable updates.
- ☐ Require peer review of resolution documentation followed by service desk management sign off.

Question 1828

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 1829

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1830

Over the last year, an information security manager has performed risk assessments on multiple third-party vendors. Which of the following criteria would be MOST helpful in determining the associated level of risk applied to each vendor?

- ☐ Compensating controls in place to protect information security
- ☐ Corresponding breaches associated with each vendor
- ☒ Criticality of the service to the organization
- ☐ Compliance requirements associated with the regulation

Question 1831

An IS auditor would be concerned if the quality assurance (QA) function were found to be performing which of the following roles?

- ☒ Reviewing the code to ensure proper documentation and development practices were followed
- ☐ Submitting corrected code for issues identified through the testing process
- ☐ Evaluating whether the testing assumptions and developed code are aligned to the design criteria
- ☐ Ensuring the development methods and standards are adhered to throughout the process

Question 1832

The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- ☐ the target's management hands-on involvement.
- ☐ the target's location.
- ☒ the target's size and complexity.
- ☐ the target's budget.
- ☐ the target's head count.
- ☐ None of the choices.

Explanation:

Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

Licensed to Berend Post berend.post@it-university.nl

Question 1833

To minimize the cost of a software project, quality management techniques should be applied:

- ☐ as close to their writing (i.e., point of origination) as possible.
- ☐ primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
- ☒ continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
- ☐ mainly at project close-down to capture lessons learned that can be applied to future projects.

Explanation:

Explanation:

While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

Question 1834

An IS auditor performing an application development review attends development team meetings. The IS auditor's independence will be compromised if the IS auditor:

- ☐ designs and executes the user's acceptance test plan.
- ☒ re-performs test procedures used by the development team.
- ☐ reviews the result of systems tests that were performed by the development team.
- ☐ assists in developing an integrated test facility on the system.

Question 1835

A design company has multiple name and address files for its customers in several of its independent systems. Which of the following is the BEST control to ensure that the customer name and address agree across all files?

- ☒ Use of hash totals on customer records
- ☐ Periodic review of each master file by management
- ☐ Matching of records and review of exception reports
- ☐ Use of authorized master file change forms

Licensed to Berend Post berend.post@it-university.nl

Question 1836

Which of the following is necessary to determine what would constitute a disaster for an organization?

- ☐ Backup strategy analysis
- ☐ Threat probability analysis
- ☐ Risk analysis
- ☒ Recovery strategy analysis

Question 1837

The IS department is evaluated monthly on its cost-revenue ratio, user satisfaction rate, and computer downtime. This can BEST be characterized as an application of:

- ☐ control self-assessment (CSA).
- ☒ balanced scorecard.
- ☐ value chain analysis.
- ☐ risk control framework.

Question 1838

During an integrated audit at a retail bank, an IS auditor is evaluating whether monthly service fees are appropriately charged for business accounts and waived for individual consumer accounts. Which of the following test approaches would utilize data analytics to facilitate the testing?

- ☐ Attempt to charge a monthly service fee to an individual consumer account.
- ☐ Evaluate whether user acceptance testing plans were designed and executed appropriately.
- ☒ Review customer accounts over the last year to determine whether appropriate charges were applied.
- ☐ Compare the system configuration settings with the business requirements document.

Question 1839

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

Licensed to Berend Post berend.post@it-university.nl

accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

Question 1840

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 1841

An organization has established three IT processing environments: development, test, and production. The MAJOR reason for separating the development and test environments is to:

- ☐ obtain segregation of duties between IT staff and end users.
- ☐ limit the users' access rights to the test environment.
- ☒ perform testing in a stable environment.
- ☐ protect the programs under development from unauthorized testing.

Question 1842

Which of the following methods would BEST ensure that IT strategy is in line with business strategy?

- ☐ Break-even-point analysis
- ☒ IT value analysis
- ☐ Critical path analysis
- ☐ Business impact analysis (BIA)

Question 1843

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

Licensed to Berend Post berend.post@it-university.nl

Question 1844

Which of the following security testing techniques is MOST effective in discovering unknown malicious attacks?

- ☐ Vulnerability testing
- ☐ Reverse engineering
- ☒ Penetration testing
- ☐ Sandboxing

Question 1845

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 1846

An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

- ☐ hardware configuration.
- ☐ access control software.
- ☒ ownership of intellectual property.
- ☐ application development methodology.

Explanation:

Explanation:

Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be of no real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

Question 1847

Which of the following is the MOST significant risk associated with the use of virtualization?

- ☐ Insufficient network bandwidth
- ☐ Single point of failure
- ☐ Inadequate configuration
- ☒ Performance issues of hosts

Licensed to Berend Post berend.post@it-university.nl

Question 1848

Which of the following would be MOST helpful in ensuring security procedures are followed by employees in a multinational organization?

- ☐ Security architecture review
- ☐ Regular clean desk reviews
- ☒ Comprehensive end-user training
- ☐ Regular policy updates by management

Question 1849

Which of the following components of a scheduling tool BEST prevents job failures due to insufficient system resources?

- ☐ Job dependencies
- ☐ Delayed job starts
- ☒ Exception handling
- ☐ Error alerts

Question 1850

An organization uses a web server hosting critical applications. Which of the following would represent the HIGHEST risk regarding the availability and integrity of the web server?

- ☐ Inadequate rotation of backups
- ☐ Not disabling the server's external drives
- ☒ Not applying program fixes on a regular basis
- ☐ Placing the web server in the DMZ

Question 1851

An organization is considering using production data for testing a new application’s functionality. Which of the following data protection techniques would BEST ensure that personal data cannot be inadvertently recovered in test environments while also reducing the need for strict confidentiality of the data?

- ☒ Data anonymization
- ☐ Data minimization
- ☐ Data normalization
- ☐ Data encryption

Licensed to Berend Post berend.post@it-university.nl

Question 1852

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 1853

Which of the following is MOST important to include in forensic data collection and preservation procedures?

- ☐ Maintaining chain of custody
- ☒ Preserving data integrity
- ☐ Determining tools to be used
- ☐ Assuring the physical security of devices

Question 1854

What should be done to determine the appropriate level of audit coverage for an organization's IT environment?

- ☐ determine the company's quarterly budget requirement.
- ☒ define an effective assessment methodology.
- ☐ calculate the company's yearly budget requirement.
- ☐ define an effective system upgrade methodology.
- ☐ define an effective network implementation methodology.

Explanation:

Explanation:

To determine the appropriate level of audit coverage for the organization's IT environment, you must define an effective assessment methodology and provide objective information to prioritize the allocation of audit resources properly.

Question 1855

An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

- ☐ tested every six months.
- ☒ regularly reviewed and updated.
- ☐ approved by the chief executive officer (CEO).
- ☐ communicated to every department head in the organization.

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

The plan should be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel. Otherwise, it may become out of date and may no longer be effective. The plan must be subjected to regular testing, but the period between tests will again depend on the nature of the organization and the relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. Similarly, although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communications staff.

Question 1856

An organization allows employees to use personally owned mobile devices to access customers' personal information. An IS auditor's GREATEST concern should be whether:

- ☐ mobile devices are compatible with company infrastructure.
- ☐ devices have the capability to segregate business and personal data.
- ☒ mobile device security policies have been implemented.
- ☐ devices have adequate storage and backup capabilities.

Question 1857

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.

Licensed to Berend Post berend.post@it-university.nl

Question 1858

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 1859

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:

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:

Licensed to Berend Post berend.post@it-university.nl

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:

All other choices presented were incorrect answers because they are not valid policies.

Reference:

CISA review manual 2014 Page number 331 and 332

Question 1860

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:

Licensed to Berend Post berend.post@it-university.nl

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 1861

Requiring that passwords contain a combination of numeric and alphabetic characters is MOST effective against which type of attack?

- ☐ Denial of service
- ☒ Dictionary
- ☐ Social engineering
- ☐ Programmed

Question 1862

An IS auditor is involved in the user testing phase of a development project. The developers wish to use a copy of a peak volume transaction file from the production process to show that the development can cope with the required volume. What is the auditor's PRIMARY concern?

- ☒ Sensitive production data may be read by unauthorized persons.
- ☐ The error-handling and credibility checks may not be fully proven.
- ☐ Users may not wish for production data to be made available for testing.
- ☐ All functionality of the new process may not be tested.

Question 1863

Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☒ Frame and bits

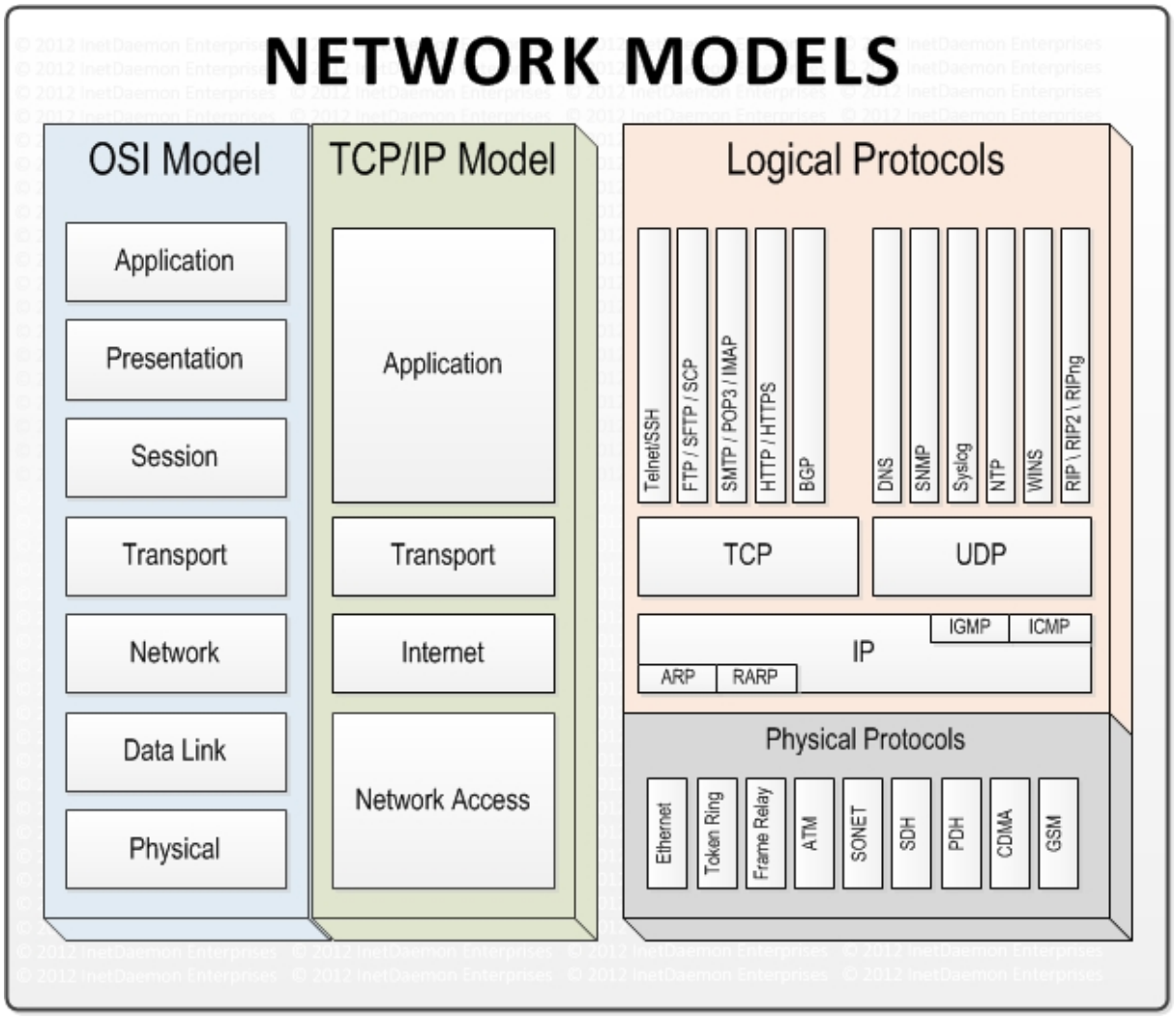
Explanation:

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.

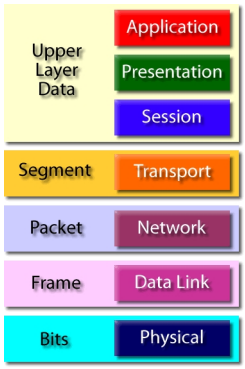
The most popular LAN architecture among those listed above is Ethernet. Ethernet uses an Access Method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to access the media, when Ethernet operates in a shared media. An Access Method determines how a host will place data on the medium.

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):



The following answers are incorrect:

Data – Application layer data PDU

Segment – Transport layer data PDU

Packet – Network interface layer data PDU

Reference:

CISA review manual 2014 page number 272

Question 1864

A month after a company purchased and implemented system and performance monitoring software, reports were too large and therefore were not reviewed or acted upon. The MOST effective plan of action would be to:

- ☒ use analytical tools to produce exception reports from the system and performance monitoring software
- ☐ re-install the system and performance monitoring software
- ☐ evaluate replacement systems and performance monitoring software
- ☐ restrict functionality of system monitoring software to security-related events

Licensed to Berend Post berend.post@it-university.nl