Isaca CISA

Certified Information Systems Auditor

Version: 3.9

Topic 1, Main Questions (240 Main Questions)

QUESTION NO: 1

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?

A. Inadequate screen/report design facilities
B. Complex programming language subsets
C. Lack of portability across operating systems
D. Inability to perform data intensive operations

Answer: D
Explanation:
4GLs are usually not suitable for data intensive operations. Instead, they are used mainly for graphic user interface (GUI) design or as simple query/report generators.

QUESTION NO: 2

Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

A. Field checks
B. Control totals
C. Reasonableness checks
D. A before-and-after maintenance report

Answer: D
Explanation:
A before-and-after maintenance report is the best answer because a visual review would provide the most positive verification that updating was proper.

QUESTION NO: 3

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Blackbox test
B. Desk checking
C. Structured walk-through
D. Design and code

Answer: A
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.

QUESTION NO: 4

Which of the following is MOST likely to result from a business process reengineering (BPR) project?

A. An increased number of people using technology
B. Significant cost savings, through a reduction in the complexity of information technology
C. A weaker organizational structures and less accountability
D. Increased information protection (IP) risk will increase

Answer: A
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 NO: 5

Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

A. Router
B. Bridge
C. Repeater
D. Gateway

Answer: B
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 NO: 6
Which of the following is a benefit of using callback devices?

A. Provide an audit trail
B. Can be used in a switchboard environment
C. Permit unlimited user mobility
D. Allow call forwarding

Answer: A

Explanation:

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

QUESTION NO: 7

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:

A. dials back to the user machine based on the user id and password using a telephone number from its database.
B. dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.
C. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.
D. waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's database.

Answer: A

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 NO: 8

Structured programming is BEST described as a technique that:

A. provides knowledge of program functions to other programmers via peer reviews.
B. reduces the maintenance time of programs by the use of small-scale program modules.
C. makes the readable coding reflect as closely as possible the dynamic execution of the program.

D. controls the coding and testing of the high-level functions of the program in the development process.

Answer: B
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 NO: 9

Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check
B. Check digit
C. Validity check
D. Duplicate check

Answer: B
Explanation:
A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered or an incorrect, but valid, value substituted. This control is effective in detecting transposition and transcription errors.

QUESTION NO: 10

An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

A. cold site.
B. warm site.
C. dial-up site.
D. duplicate processing facility.

Answer: A
Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.

QUESTION NO: 11

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?

A. Unit testing
B. Integration testing
C. Design walk-throughs
D. Configuration management

Answer: B
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.

QUESTION NO: 12

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

A. communications handler.
B. EDI translator.
C. application interface.
D. EDI interface.

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

QUESTION NO: 13

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

A. testing stage.
B. evaluation stage.

C. maintenance stage.
D. early stages of planning.

Answer: D
Explanation:
Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

QUESTION NO: 14

Which of the following network configuration options contains a direct link between any two host machines?

A. Bus
B. Ring
C. Star
D. Completely connected (mesh)

Answer: D
Explanation:
A completely connected mesh configuration creates a direct link between any two host machines.

QUESTION NO: 15

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit
B. Existence check
C. Completeness check
D. Reasonableness check

Answer: C
Explanation:
A completeness check is used to determine if a field contains data and not zeros or blanks.

QUESTION NO: 16

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controls
D. A substantive test of the program compiler controls

Answer: B
Explanation:
A compliance test determines if controls are operating as designed and are being applied in a manner that complies with management policies and procedures. For example, if the IS auditor is concerned whether program library controls are working properly, the IS auditor might select a sample of programs to determine if the source and object versions are the same. In other words, the broad objective of any compliance test is to provide auditors with reasonable assurance that a particular control on which the auditor plans to rely is operating as the auditor perceived it in the preliminary evaluation.

QUESTION NO: 17

A data administrator is responsible for:

A. maintaining database system software.
B. defining data elements, data names and their relationship.
C. developing physical database structures.
D. developing data dictionary system software.

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

QUESTION NO: 18

A database administrator is responsible for:

A. defining data ownership.
B. establishing operational standards for the data dictionary.
C. creating the logical and physical database.
D. establishing ground rules for ensuring data integrity and security.

Answer: C
Explanation:
A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data

administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

QUESTION NO: 19

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:

A. defining the conceptual schemA.
B. defining security and integrity checks.
C. liaising with users in developing data model.
D. mapping data model with the internal schemA.

Answer: D
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 enterprisewide view of data within an organization and is the basis for deriving an end-user department data model.

QUESTION NO: 20

To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

A. the entire message and thereafter enciphering the message digest using the sender's private key.
B. any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.
C. the entire message and thereafter enciphering the message using the sender's private key.
D. the entire message and thereafter enciphering the message along with the message digest using the sender's private key.

Answer: A
Explanation:
A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the

sender's private key, not the message.

QUESTION NO: 21

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

A. digest signature.
B. electronic signature.
C. digital signature.
D. hash signature.

Answer: C
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 NO: 22

A critical function of a firewall is to act as a:

A. special router that connects the Internet to a LAN.
B. device for preventing authorized users from accessing the LAN.
C. server used to connect authorized users to private trusted network resources.
D. proxy server to increase the speed of access to authorized users.

Answer: B
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 NO: 23

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

A. Spool
B. Cluster controller
C. Protocol converter
D. Front end processor

Answer: D
Explanation:
A front-end processor is a hardware device that connects all communication lines to a central computer to relieve the central computer.

QUESTION NO: 24

The use of a GANTT chart can:

A. aid in scheduling project tasks.
B. determine project checkpoints.
C. ensure documentation standards.
D. direct the post-implementation review.

Answer: A
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 NO: 25

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

A. Gateway
B. Protocol converter
C. Front-end communication processor
D. Concentrator/multiplexor

Answer: A
Explanation:
A gateway performs the job of translating e-mail formats from one network to another so messages can make their way through all the networks.

QUESTION NO: 26

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

Answer: C
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.

QUESTION NO: 27

A hub is a device that connects:

A. two LANs using different protocols.
B. a LAN with a WAN.
C. a LAN with a metropolitan area network (MAN).
D. two segments of a single LAN.

Answer: D
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 NO: 28

A LAN administrator normally would be restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

Answer: C

Explanation:

A LAN administrator should not have programming responsibilities but may have end- user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator also may be responsible for security administration over the LAN.

QUESTION NO: 29

Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator

Answer: B

Explanation:

A modem is a device that translates data from digital to analog and back to digital.

QUESTION NO: 30

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

A. A neural network
B. Database management software
C. Management information systems
D. Computer assisted audit techniques

Answer: A

Explanation:

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

QUESTION NO: 31

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

A. duplicate check.
B. table lookup.
C. validity check.
D. parity check.

Answer: D

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 NO: 32

For which of the following applications would rapid recovery be MOST crucial?

A. Point-of-sale system
B. Corporate planning
C. Regulatory reporting
D. Departmental chargeback

Answer: A

Explanation:

A point-of-sale system is a critical online system that when inoperable will jeopardize the ability of Company.com to generate revenue and track inventory properly.

QUESTION NO: 33

The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.
B. performance of a comprehensive security control review by the IS auditor.
C. adoption of a corporate information security policy statement.
D. purchase of security access control software.

Answer: C

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 NO: 34

A malicious code that changes itself with each file it infects is called a:

A. logic bomb.
B. stealth virus.
C. trojan horse.

D. polymorphic virus.

Answer: D

Explanation:

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

QUESTION NO: 35

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?

A. Paper test
B. Post test
C. Preparedness test
D. Walk-through

Answer: C

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.

QUESTION NO: 36

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 costeffective test of the DRP?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

Answer: B

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.

QUESTION NO: 37

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

A. Relocate the shut off switch.
B. Install protective covers.
C. Escort visitors.
D. Log environmental failures.

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

QUESTION NO: 38

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?

A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.

Answer: B
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 NO: 39

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:

A. registration authority (RA).
B. issuing certification authority (CA).
C. subject CA.
D. policy management authority.

Answer: A

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 NO: 40

Which of the following is a data validation edit and control?

A. Hash totals
B. Reasonableness checks
C. Online access controls
D. Before and after image reporting

Answer: B

Explanation:

A reasonableness check is a data validation edit and control, used to ensure that data conforms to predetermined criteriA.

QUESTION NO: 41

A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness check.
B. parity check.
C. redundancy check.
D. check digits.

Answer: C

Explanation:

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of datA.

QUESTION NO: 42

What is the primary objective of a control self-assessment (CSA) program?

A. Enhancement of the audit responsibility
B. Elimination of the audit responsibility
C. Replacement of the audit responsibility
D. Integrity of the audit responsibility

Answer: A
Explanation: Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

QUESTION NO: 43

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?

A. True
B. False

Answer: A
Explanation: IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

QUESTION NO: 44

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

A. The same value.
B. Greater value.
C. Lesser value.
D. Prior audit reports are not relevant.

Answer: C
Explanation: Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

QUESTION NO: 45

What is the PRIMARY purpose of audit trails?

A. To document auditing efforts
B. To correct data integrity errors
C. To establish accountability and responsibility for processed transactions
D. To prevent unauthorized access to data

Answer: C

Explanation: The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

QUESTION NO: 46

How does the process of systems auditing benefit from using a risk-based approach to audit planning?

A. Controls testing starts earlier.
B. Auditing resources are allocated to the areas of highest concern.
C. Auditing risk is reduced.
D. Controls testing is more thorough.

Answer: B

Explanation: Allocation of auditing resources to the areas of highest concern is a benefit of a risk-based approach to audit planning.

QUESTION NO: 47

After an IS auditor has identified threats and potential impacts, the auditor should:

A. Identify and evaluate the existing controls
B. Conduct a business impact analysis (BIA)
C. Report on existing controls
D. Propose new controls

Answer: A

Explanation: After an IS auditor has identified threats and potential impacts, the auditor should then identify and evaluate the existing controls.

QUESTION NO: 48

The use of statistical sampling procedures helps minimize:

A. Detection risk
B. Business risk
C. Controls risk

D. Compliance risk

Answer: A

Explanation: The use of statistical sampling procedures helps minimize detection risk.

QUESTION NO: 49

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?

A. Business risk
B. Detection risk
C. Residual risk
D. Inherent risk

Answer: B

Explanation: Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

QUESTION NO: 50

A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

A. Identify high-risk areas that might need a detailed review later
B. Reduce audit costs
C. Reduce audit time
D. Increase audit accuracy

Answer: C

Explanation: A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can identify high-risk areas that might need a detailed review later.

QUESTION NO: 51

What type of approach to the development of organizational policies is often driven by risk assessment?

A. Bottom-up
B. Top-down
C. Comprehensive
D. Integrated

Answer: B

Explanation: A bottom-up approach to the development of organizational policies is often driven by risk assessment.

QUESTION NO: 52

Who is accountable for maintaining appropriate security measures over information assets?

A. Data and systems owners
B. Data and systems users
C. Data and systems custodians
D. Data and systems auditors

Answer: A

Explanation: Data and systems owners are accountable for maintaining appropriate security measures over information assets.

QUESTION NO: 53

Proper segregation of duties prohibits a system analyst from performing quality-assurance functions. True or false?

A. True
B. False

Answer: A

Explanation: Proper segregation of duties prohibits a system analyst from performing quality-assurance functions.

QUESTION NO: 54

What should an IS auditor do if he or she observes that project-approval procedures do not exist?

A. Advise senior management to invest in project-management training for the staff
B. Create project-approval procedures for future project implementations
C. Assign project leaders
D. Recommend to management that formal approval procedures be adopted and documented

Answer: D

Explanation: If an IS auditor observes that project-approval procedures do not exist, the IS auditor should recommend to management that formal approval procedures be adopted and documented.

QUESTION NO: 55

Who is ultimately accountable for the development of an IS security policy?

A. The board of directors
B. Middle management
C. Security administrators
D. Network administrators

Answer: A

Explanation: The board of directors is ultimately accountable for the development of an IS security policy.

QUESTION NO: 56

Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

A. True
B. False

Answer: B

Explanation: Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

QUESTION NO: 57

A core tenant of an IS strategy is that it must:

A. Be inexpensive
B. Be protected as sensitive confidential information
C. Protect information confidentiality, integrity, and availability
D. Support the business objectives of the organization

Answer: D

Explanation: Above all else, an IS strategy must support the business objectives of the organization.

QUESTION NO: 58

Batch control reconciliation is a _______________________ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

A. Detective

B. Corrective
C. Preventative
D. Compensatory

Answer: D

Explanation: Batch control reconciliations is a compensatory control for mitigating risk of inadequate segregation of duties.

QUESTION NO: 59

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

A. Data is entered correctly
B. Only authorized cryptographic keys are used
C. Input is authorized
D. Database indexing is performed properly

Answer: A

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

QUESTION NO: 60

If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

A. IT cannot be implemented if senior management is not committed to strategic planning.
B. More likely.
C. Less likely.
D. Strategic planning does not affect the success of a company's implementation of IT.

Answer: C

Explanation: A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

QUESTION NO: 61

Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

A. Lack of employee awareness of a company's information security policy
B. Failure to comply with a company's information security policy
C. A momentary lapse of reason

D. Lack of security policy enforcement procedures

Answer: A

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

QUESTION NO: 62

What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

A. A star network topology
B. A mesh network topology with packet forwarding enabled at each host
C. A bus network topology
D. A ring network topology

Answer: B

Explanation: A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance.

QUESTION NO: 63

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

A. Evidence collected through personal observation
B. Evidence collected through systems logs provided by the organization's security administration
C. Evidence collected through surveys collected from internal staff
D. Evidence collected through transaction reports provided by the organization's IT administration

Answer: A

Explanation: An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

QUESTION NO: 64

What kind of protocols does the OSI Transport Layer of the TCP/IP protocol suite provide to ensure reliable communication?

A. Nonconnection-oriented protocols
B. Connection-oriented protocols
C. Session-oriented protocols

D. Nonsession-oriented protocols

Answer: B

Explanation: The transport layer of the TCP/IP protocol suite provides for connection-oriented protocols to ensure reliable communication.

QUESTION NO: 65

How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

A. EDI usually decreases the time necessary for review.
B. EDI usually increases the time necessary for review.
C. Cannot be determined.
D. EDI does not affect the time necessary for review.

Answer: A

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 NO: 66

What would an IS auditor expect to find in the console log? Choose the BEST answer.

A. Evidence of password spoofing
B. System errors
C. Evidence of data copy activities
D. Evidence of password sharing

Answer: B

Explanation: An IS auditor can expect to find system errors to be detailed in the console log.

QUESTION NO: 67

Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

Answer: A

Explanation: Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing.

QUESTION NO: 68

Why does the IS auditor often review the system logs?

A. To get evidence of password spoofing
B. To get evidence of data copy activities
C. To determine the existence of unauthorized access to data by a user or program
D. To get evidence of password sharing

Answer: C

Explanation: When trying to determine the existence of unauthorized access to data by a user or program, the IS auditor will often review the system logs.

QUESTION NO: 69

What is essential for the IS auditor to obtain a clear understanding of network management?

A. Security administrator access to systems
B. Systems logs of all hosts providing application services
C. A graphical map of the network topology
D. Administrator access to systems

Answer: C

Explanation: A graphical interface to the map of the network topology is essential for the IS auditor to obtain a clear understanding of network management.

QUESTION NO: 70

How is risk affected if users have direct access to a database at the system level?

A. Risk of unauthorized access increases, but risk of untraceable changes to the database decreases.
B. Risk of unauthorized and untraceable changes to the database increases.
C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increases.
D. Risk of unauthorized and untraceable changes to the database decreases.

Answer: B

Explanation: If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases.

QUESTION NO: 71

What is the most common purpose of a virtual private network implementation?

A. 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.
B. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connection.
C. 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.
D. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connection.

Answer: A

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 NO: 72

What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

A. The software can dynamically readjust network traffic capabilities based upon current usage.
B. The software produces nice reports that really impress management.
C. It allows users to properly allocate resources and ensure continuous efficiency of operations.
D. It allows management to properly allocate resources and ensure continuous efficiency of operations.

Answer: D

Explanation: Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

QUESTION NO: 73

What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

A. Network-monitoring software
B. A system downtime log
C. Administration activity reports
D. Help-desk utilization trend reports

Answer: B

Explanation: A system downtime log can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program.

QUESTION NO: 74

What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information? Choose the BEST answer.

A. Referential integrity controls
B. Normalization controls
C. Concurrency controls
D. Run-to-run totals

Answer: A

Explanation: Concurrency controls are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information.

QUESTION NO: 75

What increases encryption overhead and cost the most?

A. A long symmetric encryption key
B. A long asymmetric encryption key
C. A long Advance Encryption Standard (AES) key
D. A long Data Encryption Standard (DES) key

Answer: B

Explanation: A long asymmetric encryption key (public key encryption) increases encryption overhead and cost. All other answers are single shared symmetric keys.

QUESTION NO: 76

Which of the following best characterizes "worms"?

A. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
B. Programming code errors that cause a program to repeatedly dump data
C. Malicious programs that require the aid of a carrier program such as email
D. Malicious programs that masquerade as common applications such as screensavers or macro-enabled Word documents

Answer: A

Explanation: Worms are malicious programs that can run independently and can propagate without the aid of a carrier program such as email.

QUESTION NO: 77

What is an initial step in creating a proper firewall policy?

A. Assigning access to users according to the principle of least privilege
B. Determining appropriate firewall hardware and software
C. Identifying network applications such as mail, web, or FTP servers
D. Configuring firewall access rules

Answer: C
Explanation: Identifying network applications such as mail, web, or FTP servers to be externally accessed is an initial step in creating a proper firewall policy.

QUESTION NO: 78

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

A. With public-key encryption, or symmetric encryption
B. With public-key encryption, or asymmetric encryption
C. With shared-key encryption, or symmetric encryption
D. With shared-key encryption, or asymmetric encryption

Answer: B
Explanation: With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

QUESTION NO: 79

How does the SSL network protocol provide confidentiality?

A. Through symmetric encryption such as RSA
B. Through asymmetric encryption such as Data Encryption Standard, or DES
C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
D. Through symmetric encryption such as Data Encryption Standard, or DES

Answer: D
Explanation: The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption Standard, or DES.

QUESTION NO: 80

What are used as the framework for developing logical access controls?

A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)
D. Organizational charts for identifying roles and responsibilities

Answer: A

Explanation: Information systems security policies are used as the framework for developing logical access controls.

QUESTION NO: 81

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

A. Concurrency controls
B. Reasonableness checks
C. Time stamps
D. Referential integrity controls

Answer: C

Explanation: Time stamps are an effective control for detecting duplicate transactions such as payments made or received.

QUESTION NO: 82

Which of the following is a good control for protecting confidential data residing on a PC?

A. Personal firewall
B. File encapsulation
C. File encryption
D. Host-based intrusion detection

Answer: C

Explanation: File encryption is a good control for protecting confidential data residing on a PC.

QUESTION NO: 83

Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model

B. Access is granted on a least-privilege basis, per the organization's data owners
C. Implementing the Take-Grant access control model
D. Classifying data according to the subject's requirements

Answer: B

Explanation: Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

QUESTION NO: 84

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

A. A combination of public-key cryptography and digital certificates and two-factor authentication
B. A combination of public-key cryptography and two-factor authentication
C. A combination of public-key cryptography and digital certificates
D. A combination of digital certificates and two-factor authentication

Answer: C

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 NO: 85

Which of the following do digital signatures provide?

A. Authentication and integrity of data
B. Authentication and confidentiality of data
C. Confidentiality and integrity of data
D. Authentication and availability of data

Answer: A

Explanation: The primary purpose of digital signatures is to provide authentication and integrity of datA.

QUESTION NO: 86

Regarding digital signature implementation, which of the following answers is correct?

A. 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.

B. 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.
C. 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.
D. 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.

Answer: C

Explanation: A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

QUESTION NO: 87

Which of the following would provide the highest degree of server access control?

A. A mantrap-monitored entryway to the server room
B. Host-based intrusion detection combined with CCTV
C. Network-based intrusion detection
D. A fingerprint scanner facilitating biometric access control

Answer: D

Explanation: A fingerprint scanner facilitating biometric access control can provide a very high degree of server access control.

QUESTION NO: 88

What are often the primary safeguards for systems software and data?

A. Administrative access controls
B. Logical access controls
C. Physical access controls
D. Detective access controls

Answer: B

Explanation: Logical access controls are often the primary safeguards for systems software and datA. **QUESTION NO:** 89.
Which of the following is often used as a detection and deterrent control against Internet attacks?
A. Honeypots

B. CCTV

C. VPN

D. VLAN

Answer: A

Honeypots are often used as a detection and deterrent control against Internet attacks.

QUESTION NO: 89

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

A. A monitored double-doorway entry system
B. A monitored turnstile entry system
C. A monitored doorway entry system
D. A one-way door that does not allow exit after entry

Answer: A

Explanation: A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used as a deterrent control for the vulnerability of piggybacking.

QUESTION NO: 90

Which of the following is an effective method for controlling downloading of files via FTP? Choose the BEST answer.

A. An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
B. An application-layer gateway, or proxy firewall
C. A circuit-level gateway
D. A first-generation packet-filtering firewall

Answer: B

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 NO: 91

Which of the following provides the strongest authentication for physical access control?

A. Sign-in logs
B. Dynamic passwords
C. Key verification
D. Biometrics

Answer: D

Explanation: Biometrics can be used to provide excellent physical access control.

QUESTION NO: 92

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

A. Employee security awareness training
B. Administrator alerts
C. Screensaver passwords
D. Close supervision

Answer: C

Explanation: Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off.

QUESTION NO: 93

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

A. OSI Layer 2 switches with packet filtering enabled
B. Virtual Private Networks
C. Access Control Lists (ACL)
D. Point-to-Point Tunneling Protocol

Answer: C

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

QUESTION NO: 94

What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentiality.
B. Hashing algorithms are irreversible.
C. Encryption algorithms ensure data integrity.
D. Encryption algorithms are not irreversible.

Answer: B

Explanation: A key distinction between encryption and hashing algorithms is that hashing algorithms are irreversible.

QUESTION NO: 95

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

A. Data diddling
B. Skimming
C. Data corruption
D. Salami attack

Answer: A
Explanation: Data diddling involves modifying data before or during systems data entry.

QUESTION NO: 96

Which of the following is used to evaluate biometric access controls?

A. FAR
B. EER
C. ERR
D. FRR

Answer: B
Explanation: When evaluating biometric access controls, a low equal error rate (EER) is preferred. EER is also called the crossover error rate (CER).

QUESTION NO: 97

Who is ultimately responsible and accountable for reviewing user access to systems?

A. Systems security administrators
B. Data custodians
C. Data owners
D. Information systems auditors

Answer: C
Explanation: Data owners are ultimately responsible and accountable for reviewing user access to systems.

QUESTION NO: 98

Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

A. Assigning user access privileges
B. Developing organizational security policies
C. Creating roles and responsibilities
D. Classifying data

Answer: D

Explanation: To properly implement data classification, establishing data ownership is an important first step.

QUESTION NO: 99

Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

A. End-user involvement
B. Senior management involvement
C. Security administration involvement
D. IS auditing involvement

Answer: A

Explanation: End-user involvement is critical during the business impact assessment phase of business continuity planning.

QUESTION NO: 100

What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

A. Paper
B. Preparedness
C. Walk-through
D. Parallel

Answer: B

Explanation: Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

QUESTION NO: 101

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

A. Cold-site facilities
B. Disaster recovery for networks
C. Diverse processing
D. Disaster recovery for systems

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

QUESTION NO: 102

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

A. Parallel
B. Preparedness
C. Walk-thorough
D. Paper

Answer: C
Explanation: Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

QUESTION NO: 103

What influences decisions regarding criticality of assets?

A. The business criticality of the data to be protected
B. Internal corporate politics
C. The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
D. The business impact analysis

Answer: C
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 NO: 104

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

A. Cold site
B. Alternate site
C. Hot site
D. Warm site

Answer: A
Explanation: Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

QUESTION NO: 105

With the objective of mitigating the risk and impact of a major business interruption, a disasterrecovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

A. True
B. False

Answer: A
Explanation: With the objective of mitigating the risk and impact of a major business interruption, a disaster-recovery plan should endeavor to reduce the length of recovery time necessary and the costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs.

QUESTION NO: 106

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?

A. Cold site
B. Hot site
C. Alternate site
D. Warm site

Answer: A

Explanation: A cold site is often an acceptable solution for preparing for recovery of noncritical systems and datA.

QUESTION NO: 107

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.

A. IT strategic plan
B. Business continuity plan
C. Business impact analysis
D. Incident response plan

Answer: B

Explanation: Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

QUESTION NO: 108

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _______________. (fill-in-the-blank)

A. Security administrator
B. Systems auditor
C. Board of directors
D. Financial auditor

Answer: C

Explanation: Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the board of directors.

QUESTION NO: 109

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

A. True
B. False

Answer: A

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

QUESTION NO: 110

Library control software restricts source code to:

A. Read-only access
B. Write-only access
C. Full access
D. Read-write access

Answer: A

Explanation: Library control software restricts source code to read-only access.

QUESTION NO: 111

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

A. In program development and change management
B. In program feasibility studies
C. In program development
D. In change management

Answer: A

Explanation: Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

QUESTION NO: 112

What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

A. Configuring software
B. Planning security
C. Determining time and resource requirements
D. Configuring hardware

Answer: C

Explanation: Determining time and resource requirements for an application-development project is often the most difficult part of initial efforts in application development.

QUESTION NO: 113

What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively

Answer: C

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 NO: 114

Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

A. Interface systems with other applications or systems
B. The entire program, including any interface systems with other applications or systems
C. All programs, including interface systems with other applications or systems
D. Mission-critical functions and any interface systems with other applications or systems

Answer: B

Explanation: Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

QUESTION NO: 115

The quality of the metadata produced from a data warehouse is ________________ in the warehouse's design. Choose the BEST answer.

A. Often hard to determine because the data is derived from a heterogeneous data environment
B. The most important consideration
C. Independent of the quality of the warehoused databases
D. Of secondary importance to data warehouse content

Answer: B

Explanation: The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

QUESTION NO: 116

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?

A. True
B. False

Answer: B

Explanation: Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

QUESTION NO: 117

Who assumes ownership of a systems-development project and the resulting system?

A. User management
B. Project steering committee
C. IT management
D. Systems developers

Answer: A

Explanation: User management assumes ownership of a systems-development project and the resulting system.

QUESTION NO: 118

If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

A. Documentation development
B. Comprehensive integration testing
C. Full unit testing
D. Full regression testing

Answer: B

Explanation: If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further comprehensive integration testing.

QUESTION NO: 119

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?

A. True
B. False

Answer: B

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 NO: 120

What is a reliable technique for estimating the scope and cost of a software-development project?

A. Function point analysis (FPA)
B. Feature point analysis (FPA)
C. GANTT
D. PERT

Answer: A

Explanation: A function point analysis (FPA) is a reliable technique for estimating the scope and cost of a software-development project.

QUESTION NO: 121

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

A. Function Point Analysis (FPA)
B. GANTT
C. Rapid Application Development (RAD)
D. PERT

Answer: D

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

QUESTION NO: 122

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

A. Lack of IT documentation is not usually material to the controls tested in an IT audit.

B. The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.
C. 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.
D. 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.

Answer: C
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 NO: 123

What often results in project scope creep when functional requirements are not defined as well as they could be?

A. Inadequate software baselining
B. Insufficient strategic planning
C. Inaccurate resource allocation
D. Project delays

Answer: A
Explanation: Inadequate software baselining often results in project scope creep because functional requirements are not defined as well as they could be.

QUESTION NO: 124

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?

A. True
B. False

Answer: A
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 NO: 125

Run-to-run totals can verify data through which stage(s) of application processing?

A. Initial
B. Various
C. Final
D. Output

Answer: B
Explanation: Run-to-run totals can verify data through various stages of application processing.

QUESTION NO: 126

_________________ (fill in the blank) is/are are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

A. Data custodians
B. The board of directors and executive officers
C. IT security administration
D. Business unit managers

Answer: B
Explanation: The board of directors and executive officers are ultimately accountable for the functionality, reliability, and security within IT governance.

QUESTION NO: 127

What can be used to help identify and investigate unauthorized transactions? Choose the BEST answer.

A. Postmortem review
B. Reasonableness checks
C. Data-mining techniques
D. Expert systems

Answer: C
Explanation: Data-mining techniques can be used to help identify and investigate unauthorized transactions.

QUESTION NO: 128

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

A. True
B. False

Answer: A

Explanation: Network environments often add to the complexity of program-to-program communication, making application systems implementation and maintenance more difficult.

QUESTION NO: 129

______________ 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.

A. Quantitative; qualitative
B. Qualitative; quantitative
C. Residual; subjective
D. Quantitative; subjective

Answer: A

Explanation: Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

QUESTION NO: 130

What must an IS auditor understand before performing an application audit? Choose the BEST answer.

A. The potential business impact of application risks.
B. Application risks must first be identified.
C. Relative business processes.
D. Relevant application risks.

Answer: C

Explanation: An IS auditor must first understand relative business processes before performing an application audit.

QUESTION NO: 131

What is the first step in a business process re-engineering project?

A. Identifying current business processes
B. Forming a BPR steering committee
C. Defining the scope of areas to be reviewed
D. Reviewing the organizational strategic plan

Answer: C

Explanation: Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

QUESTION NO: 132

When storing data archives off-site, what must be done with the data to ensure data completeness?

A. The data must be normalized.
B. The data must be validated.
C. The data must be parallel-tested.
D. The data must be synchronized.

Answer: D

Explanation: When storing data archives off-site, data must be synchronized to ensure data completeness.

QUESTION NO: 133

Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

A. Redundancy check
B. Completeness check
C. Accuracy check
D. Parity check

Answer: A

Explanation: A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of datA.

QUESTION NO: 134

What is an edit check to determine whether a field contains valid data?

A. Completeness check
B. Accuracy check

C. Redundancy check
D. Reasonableness check

Answer: A

Explanation: A completeness check is an edit check to determine whether a field contains valid datA.

QUESTION NO: 135

A transaction journal provides the information necessary for detecting unauthorized _____________ (fill in the blank) from a terminal.

A. Deletion
B. Input
C. Access
D. Duplication

Answer: B

Explanation: A transaction journal provides the information necessary for detecting unauthorized input from a terminal.

QUESTION NO: 136

An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

A. True
B. False

Answer: B

Explanation: An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

QUESTION NO: 137

When are benchmarking partners identified within the benchmarking process?

A. In the design stage
B. In the testing stage
C. In the research stage
D. In the development stage

Answer: C

Explanation: Benchmarking partners are identified in the research stage of the benchmarking process.

QUESTION NO: 138

A check digit is an effective edit check to:

A. Detect data-transcription errors
B. Detect data-transposition and transcription errors
C. Detect data-transposition, transcription, and substitution errors
D. Detect data-transposition errors

Answer: B
Explanation: A check digit is an effective edit check to detect data-transposition and transcription errors.

QUESTION NO: 139

Parity bits are a control used to validate:

A. Data authentication
B. Data completeness
C. Data source
D. Data accuracy

Answer: B
Explanation: Parity bits are a control used to validate data completeness.

QUESTION NO: 140

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

A. Implementor
B. Facilitator
C. Developer
D. Sponsor

Answer: B
Explanation: The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

QUESTION NO: 141

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

A. Proper authentication
B. Proper identification AND authentication
C. Proper identification
D. Proper identification, authentication, AND authorization

Answer: B

Explanation: If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

QUESTION NO: 142

Which of the following is the MOST critical step in planning an audit?

A. Implementing a prescribed auditing framework such as COBIT
B. Identifying current controls
C. Identifying high-risk audit targets
D. Testing controls

Answer: C

Explanation: In planning an audit, the most critical step is identifying the areas of high risk.

QUESTION NO: 143

To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

A. The business objectives of the organization
B. The effect of segregation of duties on internal controls
C. The point at which controls are exercised as data flows through the system
D. Organizational control policies

Answer: C

Explanation: When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

QUESTION NO: 144

What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Answer: D

Explanation: When implementing continuous-monitoring systems, an IS auditor's first step is to identify highrisk areas within the organization.

QUESTION NO: 145

What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

A. Business risk
B. Audit risk
C. Detective risk
D. Inherent risk

Answer: D

Explanation: Inherent risk is associated with authorized program exits (trap doors).

QUESTION NO: 146

Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software
B. Generalized audit software
C. Productivity audit software
D. Manual review

Answer: B

Explanation: Generalized audit software can be used to search for address field duplications.

QUESTION NO: 147

Which of the following is of greatest concern to the IS auditor?

A. Failure to report a successful attack on the network
B. Failure to prevent a successful attack on the network
C. Failure to recover from a successful attack on the network
D. Failure to detect a successful attack on the network

Answer: A

Explanation: Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

QUESTION NO: 148

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated datA. True or false?

A. True
B. False

Answer: B
Explanation: An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated datA.

QUESTION NO: 149

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?

A. True
B. False

Answer: A
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 NO: 150

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?

A. To advise senior management.
B. To reassign job functions to eliminate potential fraud.
C. To implement compensator controls.
D. Segregation of duties is an administrative control not considered by an IS auditor.

Answer: A
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 NO: 151

Who is responsible for implementing cost-effective controls in an automated system?

A. Security policy administrators
B. Business unit management
C. Senior management
D. Board of directors

Answer: B

Explanation: Business unit management is responsible for implementing cost-effective controls in an automated system.

QUESTION NO: 152

Why does an IS auditor review an organization chart?

A. To optimize the responsibilities and authority of individuals
B. To control the responsibilities and authority of individuals
C. To better understand the responsibilities and authority of individuals
D. To identify project sponsors

Answer: C

Explanation: The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

QUESTION NO: 153

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

A. An IT security policies audit
B. A processing audit
C. A software audit
D. A vulnerability assessment

Answer: A

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

QUESTION NO: 154

When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

A. Ownership of the programs and files
B. A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster
C. A statement of due care
D. 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

Answer: D
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 NO: 155

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?

A. True
B. False

Answer: B
Explanation: When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

QUESTION NO: 156

What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels? Choose the BEST answer.

A. Business impact assessment
B. Risk assessment
C. IS assessment methods
D. Key performance indicators (KPIs)

Answer: C
Explanation: IS assessment methods allow IS management to determine whether the activities of the organization differ from the planned or expected levels.

QUESTION NO: 157

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.
B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
C. Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
D. Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Answer: A

Explanation: Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

QUESTION NO: 158

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

A. True
B. False

Answer: A

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

QUESTION NO: 159

Who should be responsible for network security operations?

A. Business unit managers
B. Security administrators
C. Network administrators
D. IS auditors

Answer: B

Explanation: Security administrators are usually responsible for network security operations.

QUESTION NO: 160

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

A. True
B. False

Answer: A

Explanation: Proper segregation of duties does not prohibit a quality-control administrator from also being responsible for change control and problem management.

QUESTION NO: 161

What can be implemented to provide the highest level of protection from external attack?

A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
B. Configuring the firewall as a screened host behind a router
C. Configuring the firewall as the protecting bastion host
D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Answer: A

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 NO: 162

The directory system of a database-management system describes:

A. The access method to the data
B. The location of data AND the access method
C. The location of data
D. Neither the location of data NOR the access method

Answer: B

Explanation: The directory system of a database-management system describes the location of data and the access method.

QUESTION NO: 163

How is the risk of improper file access affected upon implementing a database system?

A. Risk varies.
B. Risk is reduced.
C. Risk is not affected.
D. Risk is increased.

Answer: D

Explanation: Improper file access becomes a greater risk when implementing a database system.

QUESTION NO: 164

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

A. The data should be deleted and overwritten with binary 0s.
B. The data should be demagnetized.
C. The data should be low-level formatted.
D. The data should be deleted.

Answer: B

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

QUESTION NO: 165

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

A. The potential for unauthorized deletion of report copies
B. The potential for unauthorized modification of report copies
C. The potential for unauthorized printing of report copies
D. The potential for unauthorized editing of report copies

Answer: C

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

QUESTION NO: 166

Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

A. WAP is often configured by default settings and is thus insecure.

B. WAP provides weak encryption for wireless traffic.
C. WAP functions as a protocol-conversion gateway for wireless TLS to Internet SSL.
D. WAP often interfaces critical IT systems.

Answer: C
Explanation: Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL, the WAP gateway is a component warranting critical concern and review for the IS auditor when auditing and testing controls that enforce message confidentiality.

QUESTION NO: 167

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Answer: A
Explanation: Proper segregation of duties prevents a computer operator (user) from performing security administration duties.

QUESTION NO: 168

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

A. Modems convert analog transmissions to digital, and digital transmission to analog.
B. Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
C. Modems convert digital transmissions to analog, and analog transmissions to digital.
D. Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Answer: A
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 NO: 169

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? Choose the BEST answer.

A. Expert systems
B. Neural networks
C. Integrated synchronized systems
D. Multitasking applications

Answer: B

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

QUESTION NO: 170

What supports data transmission through split cable facilities or duplicate cable facilities?

A. Diverse routing
B. Dual routing
C. Alternate routing
D. Redundant routing

Answer: A

Explanation: Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

QUESTION NO: 171

What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

A. A first-generation packet-filtering firewall
B. A circuit-level gateway
C. An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
D. An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Answer: C

Explanation: An application-layer gateway, or proxy firewall, and stateful-inspection firewalls provide the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic.

QUESTION NO: 172

Which of the following can degrade network performance? Choose the BEST answer.

A. Superfluous use of redundant load-sharing gateways
B. Increasing traffic collisions due to host congestion by creating new collision domains

C. Inefficient and superfluous use of network devices such as switches
D. Inefficient and superfluous use of network devices such as hubs

Answer: D
Explanation: Inefficient and superfluous use of network devices such as hubs can degrade network performance.

QUESTION NO: 173

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

A. Automated electronic journaling and parallel processing
B. Data mirroring and parallel processing
C. Data mirroring
D. Parallel processing

Answer: B
Explanation: Data mirroring and parallel processing are both used to provide near-immediate recoverability for time-sensitive systems and transaction processing.

QUESTION NO: 174

What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

A. Creating user accounts that automatically expire by a predetermined date
B. Creating permanent guest accounts for temporary use
C. Creating user accounts that restrict logon access to certain hours of the day
D. Creating a single shared vendor administrator account on the basis of least-privileged access

Answer: A
Explanation: Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

QUESTION NO: 175

Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack? Choose the BEST answer.

A. Inbound traffic filtering
B. Using access control lists (ACLs) to restrict inbound connection attempts
C. Outbound traffic filtering

D. Recentralizing distributed systems

Answer: C

Explanation: Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

QUESTION NO: 176

What is a common vulnerability, allowing denial-of-service attacks?

A. Assigning access to users according to the principle of least privilege
B. Lack of employee awareness of organizational security policies
C. Improperly configured routers and router access lists
D. Configuring firewall access rules

Answer: C

Explanation: Improperly configured routers and router access lists are a common vulnerability for denial-of-service attacks.

QUESTION NO: 177

What are trojan horse programs? Choose the BEST answer.

A. A common form of internal attack
B. Malicious programs that require the aid of a carrier program such as email
C. Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
D. A common form of Internet attack

Answer: D

Explanation: Trojan horse programs are a common form of Internet attack.

QUESTION NO: 178

What is/are used to measure and ensure proper network capacity management and availability of services? Choose the BEST answer.

A. Network performance-monitoring tools
B. Network component redundancy
C. Syslog reporting
D. IT strategic planning

Answer: A

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

QUESTION NO: 179

What can be used to gather evidence of network attacks?

A. Access control lists (ACL)
B. Intrusion-detection systems (IDS)
C. Syslog reporting
D. Antivirus programs

Answer: B

Explanation: Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

QUESTION NO: 180

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis
B. SYN flood
C. Denial of service (DoS)
D. Distributed denial of service (DoS)

Answer: A

Explanation: Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

QUESTION NO: 181

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

A. Halon gas
B. Deluge sprinklers
C. Dry-pipe sprinklers
D. Wet-pipe sprinklers

Answer: C

Explanation: Although many methods of fire suppression exist, dry-pipe sprinklers are considered to be the most environmentally friendly.

QUESTION NO: 182

What is a callback system?

A. 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.
B. It is a remote-access system whereby the user's application automatically redials the remoteaccess server if the initial connection attempt fails.
C. 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.
D. 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.

Answer: C

Explanation: A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

QUESTION NO: 183

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. A dry-pipe sprinkler system
B. A deluge sprinkler system
C. A wet-pipe system
D. A halon sprinkler system

Answer: A

Explanation: A dry-pipe sprinkler system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities.

QUESTION NO: 184

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

A. False
B. True

Answer: B

Explanation: Digital signatures require the sender to "sign" the data by encrypting the data with the sender's private key, to then be decrypted by the recipient using the sender's public key.

QUESTION NO: 185

Which of the following provides the BEST single-factor authentication?

A. Biometrics
B. Password
C. Token
D. PIN

Answer: A

Explanation: Although biometrics provides only single-factor authentication, many consider it to be an excellent method for user authentication.

QUESTION NO: 186

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

A. An organizational certificate
B. A user certificate
C. A website certificate
D. Authenticode

Answer: C

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 NO: 187

What determines the strength of a secret key within a symmetric key cryptosystem?

A. A combination of key length, degree of permutation, and the complexity of the data-encryption algorithm that uses the key
B. A combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key
C. A combination of key length and the complexity of the data-encryption algorithm that uses the key
D. Initial input vectors and the complexity of the data-encryption algorithm that uses the key

Answer: B

Explanation: The strength of a secret key within a symmetric key cryptosystem is determined by a combination of key length, initial input vectors, and the complexity of the data-encryption algorithm that uses the key.

QUESTION NO: 188

What process is used to validate a subject's identity?

A. Identification
B. Nonrepudiation
C. Authorization
D. Authentication

Answer: D

Explanation: Authentication is used to validate a subject's identity.

QUESTION NO: 189

What is often assured through table link verification and reference checks?

A. Database integrity
B. Database synchronization
C. Database normalcy
D. Database accuracy

Answer: A

Explanation: Database integrity is most often ensured through table link verification and reference checks.

QUESTION NO: 190

Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

A. Systems logs
B. Access control lists (ACL)
C. Application logs
D. Error logs

Answer: B

Explanation: IS auditors should review access-control lists (ACL) to determine user permissions that have been granted for a particular resource.

QUESTION NO: 191

What should IS auditors always check when auditing password files?

A. That deleting password files is protected
B. That password files are encrypted
C. That password files are not accessible over the network
D. That password files are archived

Answer: B

Explanation: IS auditors should always check to ensure that password files are encrypted.

QUESTION NO: 192

Using the OSI reference model, what layer(s) is/are used to encrypt data?

A. Transport layer
B. Session layer
C. Session and transport layers
D. Data link layer

Answer: C

Explanation: User applications often encrypt and encapsulate data using protocols within the OSI session layer or farther down in the transport layer.

QUESTION NO: 193

When should systems administrators first assess the impact of applications or systems patches?

A. Within five business days following installation
B. Prior to installation
C. No sooner than five business days following installation
D. Immediately following installation

Answer: B

Explanation: Systems administrators should always assess the impact of patches before installation.

QUESTION NO: 194

Which of the following is the most fundamental step in preventing virus attacks?

A. Adopting and communicating a comprehensive antivirus policy
B. Implementing antivirus protection software on users' desktop computers

C. Implementing antivirus content checking at all network-to-Internet gateways
D. Inoculating systems with antivirus code

Answer: A

Explanation: Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

QUESTION NO: 195

Which of the following is of greatest concern when performing an IS audit?

A. Users' ability to directly modify the database
B. Users' ability to submit queries to the database
C. Users' ability to indirectly modify the database
D. Users' ability to directly view the database

Answer: A

Explanation: A major IS audit concern is users' ability to directly modify the database.

QUESTION NO: 196

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

A. To identify AND prevent intrusion attempts to a network
B. To prevent intrusion attempts to a network
C. Forensic incident response
D. To identify intrusion attempts to a network

Answer: D

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

QUESTION NO: 197

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?

A. True
B. False

Answer: B

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 NO: 198

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?

A. True
B. False

Answer: A

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 NO: 199

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

A. Confidentiality
B. Integrity
C. Redundancy
D. Concurrency

Answer: C

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 NO: 200

The purpose of business continuity planning and disaster-recovery planning is to:

A. Transfer the risk and impact of a business interruption or disaster
B. Mitigate, or reduce, the risk and impact of a business interruption or disaster
C. Accept the risk and impact of a business
D. Eliminate the risk and impact of a business interruption or disaster

Answer: B

Explanation: The primary purpose of business continuity planning and disaster-recovery planning is to mitigate, or reduce, the risk and impact of a business interruption or disaster. Total elimination of risk is impossible.

QUESTION NO: 201

If a database is restored from information backed up before the last system image, which of the following is recommended?

A. The system should be restarted after the last transaction.
B. The system should be restarted before the last transaction.
C. The system should be restarted at the first transaction.
D. The system should be restarted on the last transaction.

Answer: B

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.

QUESTION NO: 202

An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

A. True
B. False

Answer: B

Explanation: An off-site processing facility should not be easily identifiable externally because easy identification would create an additional vulnerability for sabotage.

QUESTION NO: 203

Which of the following is the dominating objective of BCP and DRP?

A. To protect human life
B. To mitigate the risk and impact of a business interruption
C. To eliminate the risk and impact of a business interruption
D. To transfer the risk and impact of a business interruption

Answer: A

Explanation: Although the primary business objective of BCP and DRP is to mitigate the risk and impact of a business interruption, the dominating objective remains the protection of human life.

QUESTION NO: 204

How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

A. By implementing redundant systems and applications onsite
B. By geographically dispersing resources
C. By retaining onsite data backup in fireproof vaults
D. By preparing BCP and DRP documents for commonly identified disasters

Answer: B
Explanation: Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

QUESTION NO: 205

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?

A. True
B. False

Answer: A
Explanation: Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

QUESTION NO: 206

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? Choose the BEST answer.

A. Financial reporting
B. Sales reporting
C. Inventory reporting
D. Transaction processing

Answer: D
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 NO: 207

What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

A. Off-site remote journaling
B. Electronic vaulting
C. Shadow file processing
D. Storage area network

Answer: C

Explanation: Shadow file processing can be implemented as a recovery mechanism for extremely time-sensitive transaction processing.

QUESTION NO: 208

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.

A. Accept
B. Eliminate
C. Transfer
D. Mitigate

Answer: D

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 NO: 209

Why is a clause for requiring source code escrow in an application vendor agreement important?

A. To segregate systems development and live environments
B. To protect the organization from copyright disputes
C. To ensure that sufficient code is available when needed
D. To ensure that the source code remains available even if the application vendor goes out of business

Answer: D

Explanation: A clause for requiring source code escrow in an application vendor agreement is important to ensure that the source code remains available even if the application vendor goes out of business.

QUESTION NO: 210

What uses questionnaires to lead the user through a series of choices to reach a conclusion? Choose the BEST answer.

A. Logic trees
B. Decision trees
C. Decision algorithms
D. Logic algorithms

Answer: B
Explanation: Decision trees use questionnaires to lead the user through a series of choices to reach a conclusion.

QUESTION NO: 211

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

A. Assigning copyright to the organization
B. Program back doors
C. Source code escrow
D. Internal programming expertise

Answer: C
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 NO: 212

Who is ultimately responsible for providing requirement specifications to the software-development team?

A. The project sponsor
B. The project members
C. The project leader
D. The project steering committee

Answer: A
Explanation: The project sponsor is ultimately responsible for providing requirement specifications to the software-development team.

QUESTION NO: 213

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?

A. Contrived data
B. Independently created data
C. Live data
D. Data from previous tests

Answer: D
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 NO: 214

An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

A. Meet business objectives
B. Enforce data security
C. Be culturally feasible
D. Be financially feasible

Answer: A
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 NO: 215

Which of the following processes are performed during the design phase of the systemsdevelopment life cycle (SDLC) model?

A. Develop test plans.
B. Baseline procedures to prevent scope creep.
C. Define the need that requires resolution, and map to the major requirements of the solution.
D. Program and test the new system. The tests verify and validate what has been developed.

Answer: B
Explanation: Procedures to prevent scope creep are baselined in the design phase of the systems-development life cycle (SDLC) model.

QUESTION NO: 216

When should application controls be considered within the system-development process?

A. After application unit testing
B. After application module testing
C. After applications systems testing
D. As early as possible, even in the development of the project's functional specifications

Answer: D

Explanation: Application controls should be considered as early as possible in the system-development process, even in the development of the project's functional specifications.

QUESTION NO: 217

What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

A. Rapid application development (RAD)
B. GANTT
C. PERT
D. Decision trees

Answer: A

Explanation: Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

QUESTION NO: 218

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

A. True
B. False

Answer: A

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

QUESTION NO: 219

What kind of testing should programmers perform following any changes to an application or system?

A. Unit, module, and full regression testing
B. Module testing
C. Unit testing

D. Regression testing

Answer: A

Explanation: Programmers should perform unit, module, and full regression testing following any changes to an application or system.

QUESTION NO: 220

Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

A. PERT
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. GANTT

Answer: B

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

QUESTION NO: 221

What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

A. Lack of funding
B. Inadequate user participation during system requirements definition
C. Inadequate senior management participation during system requirements definition
D. Poor IT strategic planning

Answer: B

Explanation: Inadequate user participation during system requirements definition is the most common reason for information systems to fail to meet the needs of users.

QUESTION NO: 222

Who is responsible for the overall direction, costs, and timetables for systems-development projects?

A. The project sponsor
B. The project steering committee
C. Senior management
D. The project team leader

Answer: B

Explanation: The project steering committee is responsible for the overall direction, costs, and timetables for systems-development projects.

QUESTION NO: 223

When should plans for testing for user acceptance be prepared? Choose the BEST answer.

A. In the requirements definition phase of the systems-development project
B. In the feasibility phase of the systems-development project
C. In the design phase of the systems-development project
D. In the development phase of the systems-development project

Answer: A

Explanation: Plans for testing for user acceptance are usually prepared in the requirements definition phase of the systems-development project.

QUESTION NO: 224

Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

A. Failing to perform user acceptance testing
B. Lack of user training for the new system
C. Lack of software documentation and run manuals
D. Insufficient unit, module, and systems testing

Answer: A

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.

QUESTION NO: 225

Input/output controls should be implemented for which applications in an integrated systems environment?

A. The receiving application
B. The sending application
C. Both the sending and receiving applications
D. Output on the sending application and input on the receiving application

Answer: C

Explanation: Input/output controls should be implemented for both the sending and receiving applications in an integrated systems environment

QUESTION NO: 226

Authentication techniques for sending and receiving data between EDI systems is crucial to prevent which of the following? Choose the BEST answer.

A. Unsynchronized transactions
B. Unauthorized transactions
C. Inaccurate transactions
D. Incomplete transactions

Answer: B

Explanation: Authentication techniques for sending and receiving data between EDI systems are crucial to prevent unauthorized transactions.

QUESTION NO: 227

After identifying potential security vulnerabilities, what should be the IS auditor's next step?

A. To evaluate potential countermeasures and compensatory controls
B. To implement effective countermeasures and compensatory controls
C. To perform a business impact analysis of the threats that would exploit the vulnerabilities
D. To immediately advise senior management of the findings

Answer: C

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 NO: 228

What is the primary security concern for EDI environments? Choose the BEST answer.

A. Transaction authentication
B. Transaction completeness
C. Transaction accuracy
D. Transaction authorization

Answer: D

Explanation: Transaction authorization is the primary security concern for EDI environments.

QUESTION NO: 229

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

A. Exposures
B. Threats
C. Hazards
D. Insufficient controls

Answer: B

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

QUESTION NO: 230

Business process re-engineering often results in _____________ automation, which results in _____________ number of people using technology. Fill in the blanks.

A. Increased; a greater
B. Increased; a fewer
C. Less; a fewer
D. Increased; the same

Answer: A

Explanation: Business process re-engineering often results in increased automation, which results in a greater number of people using technology.

QUESTION NO: 231

Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

A. True
B. False

Answer: A

Explanation: Whenever business processes have been re-engineered, the IS auditor should attempt to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes.

QUESTION NO: 232

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

A. Before transaction completion
B. Immediately after an EFT is initiated
C. During run-to-run total testing
D. Before an EFT is initiated

Answer: D
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 NO: 233

________________ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

A. Control totals
B. Authentication controls
C. Parity bits
D. Authorization controls

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

QUESTION NO: 234

What is used as a control to detect loss, corruption, or duplication of data?

A. Redundancy check
B. Reasonableness check
C. Hash totals
D. Accuracy check

Answer: C
Explanation: Hash totals are used as a control to detect loss, corruption, or duplication of datA.

QUESTION NO: 235

Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

A. Deterrent integrity controls
B. Detective integrity controls

C. Corrective integrity controls
D. Preventative integrity controls

Answer: D

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

QUESTION NO: 236

Processing controls ensure that data is accurate and complete, and is processed only through which of the following? Choose the BEST answer.

A. Documented routines
B. Authorized routines
C. Accepted routines
D. Approved routines

Answer: B

Explanation: Processing controls ensure that data is accurate and complete, and is processed only through authorized routines.

QUESTION NO: 237

What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

A. Accuracy check
B. Completeness check
C. Reasonableness check
D. Redundancy check

Answer: C

Explanation: A reasonableness check is a data validation edit control that matches input data to an occurrence rate.

QUESTION NO: 238

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

A. True
B. False

Answer: A

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

QUESTION NO: 239

An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

A. Substantive
B. Compliance
C. Integrated
D. Continuous audit

Answer: A

Explanation: Using a statistical sample to inventory the tape library is an example of a substantive test.

Topic 2, IS AUDIT PROCESS (80 PRACTICE QUESTIONS)

QUESTION NO: 240

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:

A. variable sampling.
B. substantive testing.
C. compliance testing.
D. stop-or-go sampling.

Answer: C

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 NO: 241

The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

A. Inherent
B. Detection
C. Control
D. Business

Answer: B

Explanation:

Detection risks are directly affected by the auditor's selection of audit procedures and techniques. Inherent risks are not usually affected by an IS auditor. Control risks are controlled by the actions of the company's management. Business risks are not affected by an IS auditor.

QUESTION NO: 242

Overall business risk for a particular threat can be expressed as:

A. a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
B. the magnitude of the impact should a threat source successfully exploit the vulnerability.
C. the likelihood of a given threat source exploiting a given vulnerability.
D. the collective judgment of the risk assessment team.

Answer: A

Explanation:

Choice A takes into consideration the likelihood and magnitude of the impact and provides the best measure of the risk to an asset. Choice B provides only the likelihood of a threat exploiting a vulnerability in the asset but does not provide the magnitude of the possible damage to the asset. Similarly, choice C considers only the magnitude of the damage and not the possibility of a threat exploiting a vulnerability. Choice D defines the risk on an arbitrary basis and is not suitable for a scientific risk management process.

QUESTION NO: 243

Which of the following is a substantive test?

A. Checking a list of exception reports
B. Ensuring approval for parameter changes
C. Using a statistical sample to inventory the tape library
D. Reviewing password history reports

Answer: C

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 NO: 244

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

A. scheduling may be performed months in advance.
B. budgets are more likely to be met by the IS audit staff.
C. staff will be exposed to a variety of technologies.
D. resources are allocated to the areas of highest concern

Answer: D
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 schedulingmethods. 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 NO: 245

An audit charter should:

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

Answer: D
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.

QUESTION NO: 246
The MAJOR advantage of the risk assessment approach over the baseline approach to

information security management is that it ensures:

A. information assets are overprotected.
B. a basic level of protection is applied regardless of asset value.
C. appropriate levels of protection are applied to information assets.
D. an equal proportion of resources are devoted to protecting all information assets.

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

QUESTION NO: 247

Which of the following sampling methods is MOST useful when testing for compliance?

A. Attribute sampling
B. Variable sampling
C. Stratified mean per unit
D. Difference estimation

Answer: A
Explanation:
Attribute sampling is the primary sampling method used for compliance testing. Attribute sampling is a sampling model that is used to estimate the rate of occurrence of a specific quality (attribute) in a population and is used in compliance testingto confirm whether the quality exists. The other choices are used in substantive testing, which involves testing of details or quantity.

QUESTION NO: 248

Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain available.
B. Access controls establish accountability for e-mail activity.
C. Data classification regulates what information should be communicated via e-mail.
D. Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Answer: A

Explanation:

Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

QUESTION NO: 249

An IS auditor is assigned to perform a postimplementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application system.
B. designed an embedded audit module exclusively for auditing the application system.
C. participated as a member of the application system project team, but did not have operational responsibilities.
D. provided consulting advice concerning application system best practices.

Answer: A

Explanation:

Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair an IS auditor's independence. Choice D isincorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

QUESTION NO: 250

The PRIMARY advantage of a continuous audit approach is that it:

A. does not require an IS auditor to collect evidence on system reliability while processing is taking place.
B. requires the IS auditor to review and follow up immediately on all information collected.
C. can improve system security when used in time-sharing environments that process a large number of transactions.
D. does not depend on the complexity of an organization's computer systems.

Answer: C

Explanation:

The use of continuous auditing techniques can improve system security when used in time-sharing environments that process a large number of transactions, but leave a scarce paper trail. Choice A is incorrect since the continuous audit approach oftendoes require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

QUESTION NO: 251

The PRIMARY purpose of audit trails is to:

A. improve response time for users.
B. establish accountability and responsibility for processed transactions.
C. improve the operational efficiency of the system.
D. provide useful information to auditors who may wish to track transactions

Answer: B
Explanation:
Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

QUESTION NO: 252

When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

A. controls needed to mitigate risks are in place.
B. vulnerabilities and threats are identified.
C. audit risks are considered.
D. a gap analysis is appropriate.

Answer: B
Explanation:
In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risksare in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be doneto compare the actual state to an expected or desirable state.

QUESTION NO: 253

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

A. schedule the audits and monitor the time spent on each audit.
B. train the IS audit staff on current technology used in the company.
C. develop the audit plan on the basis of a detailed risk assessment.
D. monitor progress of audits and initiate cost control measures.

Answer: C
Explanation:
Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

QUESTION NO: 254

An organization's IS audit charter should specify the:

A. short- and long-term plans for IS audit engagements
B. objectives and scope of IS audit engagements.
C. detailed training plan for the IS audit staff.
D. role of the IS audit function.

Answer: D
Explanation:
An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee. Short-term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

QUESTION NO: 255

An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

A. the controls already in place.
B. the effectiveness of the controls in place.
C. the mechanism for monitoring the risks related to the assets.
D. the threats/vulnerabilities affecting the assets.

Answer: D

Explanation:

One of the key factors to be considered while assessing the risks related to the use of various information systems is the threats and vulnerabilities affecting the assets. The risks related to the use of information assets should be evaluated in isolation from the installed controls. Similarly, the effectiveness of the controls should be considered during the risk mitigation stage and not during the risk assessment phase

A mechanism to continuously monitor the risks related to assets should be put in place during the risk monitoring function that follows the risk assessment phase.

QUESTION NO: 256

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

A. areas of high risk.
B. skill sets of the audit staff.
C. test steps in the audit.
D. time allotted for the audit.

Answer: A

Explanation:

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

QUESTION NO: 257

The extent to which data will be collected during an IS audit should be determined based on the:

A. availability of critical and required information.
B. auditor's familiarity with the circumstances.
C. auditee's ability to find relevant evidence.
D. purpose and scope of the audit being done.

Answer: D

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 thescope of the audit should not be limited by the auditee's ability to find relevant evidence.

QUESTION NO: 258

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

A. reasonable assurance that the audit will cover material items.
B. definite assurance that material items will be covered during the audit work.
C. reasonable assurance that all items will be covered by the audit.
D. sufficient assurance that all items will be covered during the audit work.

Answer: A
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 NO: 259

An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantified.
B. the auditor wishes to avoid sampling risk.
C. generalized audit software is unavailable.
D. the tolerable error rate cannot be determined.

Answer: A
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.

QUESTION NO: 260

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

A. address audit objectives.
B. collect sufficient evidence.
C. specify appropriate tests.
D. minimize audit resources.

Answer: A
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 theyare not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

QUESTION NO: 261

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

A. sufficient evidence will be collected.
B. all significant deficiencies identified will be corrected within a reasonable period.
C. all material weaknesses will be identified.
D. audit costs will be kept at a minimum level.

Answer: A
Explanation:
Procedures are processes an IS auditor may follow in an audit engagement. In determining the appropriateness of any specific procedure, an IS auditor should use professional judgment appropriate to the specific circumstances. Professional judgment involves a subjective and often qualitative evaluation of conditions arising in the course of an audit. Judgment addresses a grey area where binary (yes/no) decisions are not appropriate and the auditor's past experience plays a key role in making a judgment. ISACA's guidelines provide information on how to meet the standards when performing IS audit work. Identifying material weaknesses is the result of appropriate competence, experience and thoroughness in planning and executing the audit and not of professional judgment. Professional judgment is not a primary input to the financial aspects of the audit.

QUESTION NO: 262

An IS auditor evaluating logical access controls should FIRST:

A. document the controls applied to the potential access paths to the system.
B. test controls over the access paths to determine if they are functional.

C. evaluate the security environment in relation to written policies and practices
D. obtain an understanding of the security risks to information processing.

Answer: D
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 andevaluation 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, theIS 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 NO: 263

The PRIMARY purpose of an IT forensic audit is:

A. to participate in investigations related to corporate fraud.
B. the systematic collection of evidence after a system irregularity.
C. to assess the correctness of an organization's financial statements
D. to determine that there has been criminal activity.

Answer: B
Explanation:
Choice B describes a forensic audit. The evidence collected could then be used in judicial proceedings. Forensic audits are not limited to corporate fraud. Assessing the correctness of an organization's financial statements is not the purpose of a forensic audit. Drawing a conclusion as to criminal activity would be part of a legal process and not the objective of a forensic audit.

QUESTION NO: 264

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?

A. Issue an audit finding
B. Seek an explanation from IS management
C. Review the classifications of data held on the server
D. Expand the sample of logs reviewed

Answer: D
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 NO: 265

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?

A. CASE tools
B. Embedded data collection tools
C. Heuristic scanning tools
D. Trend/variance detection tools

Answer: D

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 NO: 266

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?

A. There are a number of external modems connected to the network.
B. Users can install software on their desktops.
C. Network monitoring is very limited.
D. Many user IDs have identical passwords.

Answer: D

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 detectabuse of user accounts in special circumstances and is, therefore, not a first line of defense.

QUESTION NO: 267

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

A. The preservation of the chain of custody for electronic evidence
B. Time and cost savings
C. Efficiency and effectiveness
D. Ability to search for violations of intellectual property rights

Answer: A
Explanation:
The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

QUESTION NO: 268

An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

A. matching control totals of the imported data to control totals of the original data.
B. sorting the data to confirm whether the data are in the same order as the original data.
C. reviewing the printout of the first 100 records of original data with the first 100 records of imported data.
D. filtering data for different categories and matching them to the original data.

Answer: A
Explanation:
Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported datA. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification andconfirms the accuracy of only these records. Filtering data for different categories and

matching them to original data would still require that control totals be developed to confirm the completeness of the data.

QUESTION NO: 269 CORRECT TEXT

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?

A) Test data

B. Generalized audit software

C. Integrated test facility

D. Embedded audit module

Answer: B

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 torecompute 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. Neitheran integrated test facility nor an embedded audit module would detect errors for a previous period.

QUESTION NO: 270

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

A. create the procedures document.
B. terminate the audit.
C. conduct compliance testing.
D. identify and evaluate existing practices.

Answer: D

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 whichto test compliance.

QUESTION NO: 271

In the course of performing a risk analysis, an IS auditor has identified threats and

potential impacts. Next, the IS auditor should:

A. identify and assess the risk assessment process used by management.
B. identify information assets and the underlying systems.
C. disclose the threats and impacts to management.
D. identify and evaluate the existing controls.

Answer: D
Explanation:
It is important for an IS auditor to identify and evaluate the existing controls and security once the potential threats and possible impacts are identified. Upon completion of an audit an IS auditor should describe and discuss with management the threats and potential impacts on the assets.

QUESTION NO: 272

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

A. Lack of reporting of a successful attack on the network
B. Failure to notify police of an attempted intrusion
C. Lack of periodic examination of access rights
D. Lack of notification to the public of an intrusion

Answer: A
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 NO: 273

Which of the following would normally be the MOST reliable evidence for an auditor?

A. A confirmation letter received from a third party verifying an account balance
B. Assurance from line management that an application is working as designed
C. Trend data obtained from World Wide Web (Internet) sources

D. Ratio analysts developed by the IS auditor from reports supplied by line management

Answer: A

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 NO: 274

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?

A. The point at which controls are exercised as data flow through the system
B. Only preventive and detective controls are relevant
C. Corrective controls can only be regarded as compensating
D. Classification allows an IS auditor to determine which controls are missing

Answer: A

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 NO: 275

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

A. Discussion with management
B. Review of the organization chart
C. Observation and interviews
D. Testing of user access rights

Answer: C

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 observationsand 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 regardingsegregation 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 NO: 276

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:

A. test data to validate data input.
B. test data to determine system sort capabilities.
C. generalized audit software to search for address field duplications.
D. generalized audit software to search for account field duplications.

Answer: C
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 NO: 277

Which of the following would be the BEST population to take a sample from when testing program changes?

A. Test library listings
B. Source program listings
C. Program change requests
D. Production library listings

Answer: D
Explanation:
The best source from which to draw any sample or test of system information is the automated system. The production libraries represent executables that are approved and authorized to process organizational datA. Source program listings would be timeintensive. Program change requests are the documents used to initiate change; there is no guarantee that the request has been completed for all changes. Test library listings do not represent the approved and authorized executables.

QUESTION NO: 278

An integrated test facility is considered a useful audit tool because it:

A. is a cost-efficient approach to auditing application controls.
B. enables the financial and IS auditors to integrate their audit tests.
C. compares processing output with independently calculated data.
D. provides the IS auditor with a tool to analyze a large range of information

Answer: C
Explanation:
An integrated test facility is considered a useful audit tool because it uses the same programs to compare processing using independently calculated datA. This involves setting up dummy entities on an application system and processing test or production data against the entity as a means of verifying processing accuracy.

QUESTION NO: 279

Data flow diagrams are used by IS auditors to:

A. order data hierarchically.
B. highlight high-level data definitions.
C. graphically summarize data paths and storage.
D. portray step-by-step details of data generation.

Answer: C
Explanation:
Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of datA. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

QUESTION NO: 280

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

A. An oral statement from the auditee
B. The results of a test performed by an IS auditor
C. An internally generated computer accounting report
D. A confirmation letter received from an outside source

Answer: D

Explanation:

Evidence obtained from outside sources is usually more reliable than that obtained from within the organization. Confirmation letters received from outside parties, such as those used to verify accounts receivable balances, are usually highly reliable. Testing performed by an auditor may not be reliable, if the auditor did not have a good understanding of the technical area under review.

QUESTION NO: 281

An IS auditor reviews an organizational chart PRIMARILY for:

A. an understanding of workflows.
B. investigating various communication channels.
C. understanding the responsibilities and authority of individuals.
D. investigating the network connected to different employees.

Answer: C

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 aboutthe 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 NO: 282

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?

A. Availability of online network documentation
B. Support of terminal access to remote hosts
C. Handling file transfer between hosts and interuser communications
D. Performance management, audit and control

Answer: A

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.

QUESTION NO: 283

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storage.
B. interview programmers about the procedures currently being followed.
C. compare utilization records to operations schedules.
D. review data file access records to test the librarian function.

Answer: B
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 NO: 284

Which of the following is an advantage of an integrated test facility (ITF)?

A. It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.
B. Periodic testing does not require separate test processes.
C. It validates application systems and tests the ongoing operation of the system.
D. The need to prepare test data is eliminated.

Answer: B
Explanation:
An integrated test facility creates a fictitious entity in the database to process test transactions simultaneously with live input. Its advantage is that periodic testing does not require separate test processes. However, careful planning is necessary, and test data must be isolated from production data.

QUESTION NO: 285

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?

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

Answer: C

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 notbe made until all results are confirmed.

QUESTION NO: 286

The BEST method of proving the accuracy of a system tax calculation is by:

A. detailed visual review and analysis of the source code of the calculation programs
B. recreating program logic using generalized audit software to calculate monthly totals.
C. preparing simulated transactions for processing and comparing the results to predetermined results.
D. automatic flowcharting and analysis of the source code of the calculation programs.

Answer: C

Explanation:

Preparing simulated transactions for processing and comparing the results to predetermined results is the best method for proving accuracy of a tax calculation. Detailed visual review, flowcharting and analysis of source code are not effective methods, and monthly totals would not address the accuracy of individual tax calculations.

QUESTION NO: 287

An IS auditor performing a review of an application's controls would evaluate the:

A. efficiency of the application in meeting the business processes.
B. impact of any exposures discovered.
C. business processes served by the application.
D. application's optimization.

Answer: B

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 anaudit restricted to a review of controls.

QUESTION NO: 288

In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

A. Testing whether inappropriate personnel can change application parameters
B. Tracing purchase orders to a computer listing
C. Comparing receiving reports to purchase order details
D. Reviewing the application documentation

Answer: A

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 thesame as what is happening.

QUESTION NO: 289

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

A. Embedded audit module
B. Integrated test facility
C. Snapshots
D. Audit hooks

Answer: D

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 audittrail is required.

QUESTION NO: 290

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

A. topology diagrams.
B. bandwidth usage.
C. traffic analysis reports.
D. bottleneck locations.

Answer: A

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 NO: 291

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

A. Observe the response mechanism.
B. Clear the virus from the network.
C. Inform appropriate personnel immediately.
D. Ensure deletion of the virus.

Answer: C
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 NO: 292

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

A. determining whether bar code readers are installed.
B. determining whether the movement of tapes is authorized.
C. conducting a physical count of the tape inventory.
D. checking if receipts and issues of tapes are accurately recorded.

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

QUESTION NO: 293

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

A. analysis.
B. evaluation.
C. preservation.
D. disclosure.

Answer: C
Explanation:
Preservation and documentation of evidence for review by law enforcement and judicial authorities are of primary concern when conducting an investigation. Failure to properly preserve the evidence could jeopardize the acceptance of the evidence in legal proceedings. Analysis, evaluation and disclosure are important but not of primary concern in a forensic investigation.

QUESTION NO: 294

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:

A. conclude that the controls are inadequate.
B. expand the scope to include substantive testing.
C. place greater reliance on previous audits.
D. suspend the audit.

Answer: B
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 NO: 295

An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

A. professional independence
B. organizational independence.
C. technical competence.
D. professional competence.

Answer: A

Explanation:

When an IS auditor recommends a specific vendor, they compromise professional independence. Organizational independence has no relevance to the content of an audit report and should be considered at the time of accepting the engagement. Technical and professional competence is not relevant to the requirement of independence.

QUESTION NO: 296

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

A. understand the business process.
B. comply with auditing standards.
C. identify control weakness.
D. plan substantive testing.

Answer: A

Explanation:

Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

QUESTION NO: 297

In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

A. examine source program changes without information from IS personnel.
B. detect a source program change made between acquiring a copy of the source and the comparison run.
C. confirm that the control copy is the current version of the production program.
D. ensure that all changes made in the current source copy are detected.

Answer: A

Explanation:

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately. Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

QUESTION NO: 298

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

A. confirm that the auditors did not overlook any important issues.
B. gain agreement on the findings.
C. receive feedback on the adequacy of the audit procedures.
D. test the structure of the final presentation.

Answer: B

Explanation:

The primary purpose for meeting with auditees prior to formally closing a review is to gain agreement on the findings. The other choices, though related to the formal closure of an audit, are of secondary importance.

QUESTION NO: 299

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?

A. Test data run
B. Code review
C. Automated code comparison
D. Review of code migration procedures

Answer: C

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 NO: 300

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

A. include the statement of management in the audit report.
B. identify whether such software is, indeed, being used by the organization.
C. reconfirm with management the usage of the software.
D. discuss the issue with senior management since reporting this could have a negative impact on

the organization.

Answer: B

Explanation:

When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

QUESTION NO: 301

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

A. audit trail of the versioning of the work papers.
B. approval of the audit phases.
C. access rights to the work papers.
D. confidentiality of the work papers.

Answer: D

Explanation:

Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

QUESTION NO: 302

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

A. comply with regulatory requirements.
B. provide a basis for drawing reasonable conclusions.
C. ensure complete audit coverage.
D. perform the audit according to the defined scope.

Answer: B

Explanation:

The scope of an IS audit is defined by its objectives. This involves identifying control weaknesses relevant to the scope of the audit. Obtaining sufficient and appropriate evidence assists the auditor in not only identifying control weaknesses but also documenting and validating them. Complying with regulatory requirements, ensuring coverage and the execution of audit are all relevant to an audit but are not the reason why sufficient and relevant evidence is required.

QUESTION NO: 303

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

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

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

QUESTION NO: 304

Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

A. Attribute sampling
B. Generalized audit software (GAS)
C. Test data
D. Integrated test facility (ITF)

Answer: B
Explanation:
Generalized audit software (GAS) would enable the auditor to review the entire invoice file to look for those items that meet the selection criteriA. Attribute sampling would aid in identifying records meeting specific conditions, but would not compare one record to another to identify duplicates. To detect duplicate invoice records the IS auditor should check all of the items that meet the criteria and not just a sample of the items. Test data are used to verify program processing, but will notidentify 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 NO: 305

Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

A. Reviewing a report of security rights in the system
B. Reviewing the complexities of authorization objects
C. Building a program to identify conflicts in authorization
D. Examining recent access rights violation cases

Answer: C
Explanation:
Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. A program could be developed to identify these conflicts. A report of security rights in the enterprise resource planning (ERP) system would be voluminous and time consuming to review; therefore, this technique is not as effective as building a program. As complexities increase, it becomes more difficult to verify the effectiveness of the systems and complexity is not, in itself, a link to segregation of duties. It is good practice to review recent access rights violation cases; however, it may require a significant amount of time to truly identify which violations actually resulted froman inappropriate segregation of duties.

QUESTION NO: 306

Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

A. System log analysis
B. Compliance testing
C. Forensic analysis
D. Analytical review

Answer: B
Explanation:
Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently. It is unlikely that the system log analysis would provide information about the modification of programs. Forensic analysis is a specialized technique for criminal investigation. An analytical review assesses the general control environment of an organization.

QUESTION NO: 307

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?

A. Recommend redesigning the change management process.
B. Gain more assurance on the findings through root cause analysis.
C. Recommend that program migration be stopped until the change process is documented.
D. Document the finding and present it to management.

Answer: B
Explanation:
A change management process is critical to IT production systems. Before recommending that the organization take any other action (e.g., stopping migrations, redesigning the change management process), the IS auditor should gain assurance that the incidents reported are related to deficiencies in the change management process and not caused by some process other than change management.

QUESTION NO: 308

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?

A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network

Answer: C
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 NO: 309

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:

A. decline the assignment.
B. inform management of the possible conflict of interest after completing the audit assignment.
C. inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
D. communicate the possibility of conflict of interest to management prior to starting the assignment.

Answer: D
Explanation:

Communicating the possibility of a conflict of interest to management prior to starting the assignment is the correct answer. A possible conflict of interest, likely to affect the auditor's independence, should be brought to the attention of management prior to starting the assignment. Declining the assignment is not the correct answer because the assignment could be accepted after obtaining management approval. Informing management of the possible conflict of interest after completion of the audit assignment is not correct because approval should be obtained prior to commencement and not after the completion of the assignment. Informing the business continuity planning (BCP) team of the possible conflict of interest prior to starting of the assignment is not the correct answer since the BCP team would not have the authority to decide on this issue.

QUESTION NO: 310

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?

A. Personally delete all copies of the unauthorized software.
B. Inform the auditee of the unauthorized software, and follow up to confirm deletion.
C. Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Answer: C

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 NO: 311

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
B. not include the finding in the final report, because the audit report should include only unresolved findings.
C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
D. include the finding in the closing meeting for discussion purposes only.

Answer: A

Explanation:

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

QUESTION NO: 312

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 beingchecked properly. While preparing the audit report, the IS auditor should:

A. record the observations separately with the impact of each of them marked against each respective finding.
B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
C. record the observations and the risk arising from the collective weaknesses.
D. apprise the departmental heads concerned with each observation and properly document it in the report.

Answer: C

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 affect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

QUESTION NO: 313

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

A. ask the auditee to sign a release form accepting full legal responsibility.
B. elaborate on the significance of the finding and the risks of not correcting it.
C. report the disagreement to the audit committee for resolution.
D. accept the auditee's position since they are the process owners.

Answer: B

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.

QUESTION NO: 314

When preparing an audit report the IS auditor should ensure that the results are supported by:

A. statements from IS management.
B. workpapers of other auditors.
C. an organizational control self-assessment.
D. sufficient and appropriate audit evidence.

Answer: D
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 NO: 315

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

A. audit committee.
B. auditee's manager.
C. IS auditor.
D. CEO of the organization

Answer: C
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 NO: 316

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

A. can identify high-risk areas that might need a detailed review later.
B. allows IS auditors to independently assess risk.
C. can be used as a replacement for traditional audits.
D. allows management to relinquish responsibility for control.

Answer: A
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.

QUESTION NO: 317

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

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

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

QUESTION NO: 318

Which of the following is an attribute of the control self-assessment (CSA) approach?

A. Broad stakeholder involvement
B. Auditors are the primary control analysts
C. Limited employee participation
D. Policy driven

Answer: A

Explanation:

The control self-assessment (CSA) approach emphasizes management of and accountability for developing and monitoring the controls of an organization's business processes. The attributes of CSA include empowered employees, continuous improvement, extensive employee participation and training, at! of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

QUESTION NO: 319

Which of the following is the key benefit of control self-assessment (CSA)?

A. Management ownership of the internal controls supporting business objectives is reinforced.
B. Audit expenses are reduced when the assessment results are an input to external audit work.
C. Improved fraud detection since internal business staff are engaged in testing controls
D. Internal auditors can shift to a consultative approach by using the results of the assessment.

Answer: A

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.

Topic 3, IT GOVERNANCE (111 PRACTICE QUESTION)

QUESTION NO: 320

An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirements.
B. if proposed system functionality is adequate.
C. the stability of existing software.
D. the complexity of installed technology.

Answer: A

Explanation:

The role of an IT steering committee is to ensure that the IS department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IS processes support the business requirements. Assessing proposed additional functionality and evaluating software stability and the complexity of technology are too narrow in scope to ensure that IT processes are, in fact, supporting the organization's goals.

QUESTION NO: 321

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technology.
B. a lack of a methodology for systems development.
C. technology not aligning with the organization's objectives.
D. an absence of control over technology contracts.

Answer: C
Explanation:
A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

QUESTION NO: 322

Which of the following is a function of an IS steering committee?

A. Monitoring vendor-controlled change control and testing
B. Ensuring a separation of duties within the information's processing environment
C. Approving and monitoring major projects, the status of IS plans and budgets
D. Liaising between the IS department and the end users

Answer: C
Explanation:
The IS steering committee typically serves as a general review board for major IS projects and should not become involved in routine operations; therefore, one of its functions is to approve and monitor major projects, the status of IS plans and budgets. Vendor change control is an outsourcing issue and should be monitored by IS management. Ensuring a separation of duties within the information's processing environment is an IS management responsibility. Liaising between the IS department and the end users is a function of the individual parties and not a committee.

QUESTION NO: 323

An IS steering committee should:

A. include a mix of members from different departments and staff levels.
B. ensure that IS security policies and procedures have been executed properly.
C. have formal terms of reference and maintain minutes of its meetings.
D. be briefed about new trends and products at each meeting by a vendor.

Answer: C
Explanation:
It is important to keep detailed steering committee minutes to document the decisions and activities of the IS steering committee, and the board of directors should be informed about those decisions on a timely basis. Choice A is incorrect because only senior management or high-level staff members should be on this committee because of its strategic mission. Choice B is not a responsibility of this committee, but the responsibility of the security administrator. Choice D is incorrect because a vendor should be invited to meetings only when appropriate.

QUESTION NO: 324

Involvement of senior management is MOST important in the development of:

A. strategic plans.
B. IS policies.
C. IS procedures.
D. standards and guidelines.

Answer: A
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 NO: 325

Effective IT governance will ensure that the IT plan is consistent with the organization's:

A. business plan.
B. audit plan.
C. security plan.
D. investment plan.

Answer: A
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 NO: 326

Establishing the level of acceptable risk is the responsibility of:

A. quality assurance management.
B. senior business management.
C. the chief information officer.
D. the chief security officer.

Answer: B
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.

QUESTION NO: 327

IT governance is PRIMARILY the responsibility of the:

A. chief executive officer.
B. board of directors.
C. IT steering committee.
D. audit committee.

Answer: B
Explanation:
IT governance is primarily the responsibility of the executives and shareholders {as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

QUESTION NO: 328

As an outcome of information security governance, strategic alignment provides:

A. security requirements driven by enterprise requirements.
B. baseline security following best practices.
C. institutionalized and commoditized solutions.
D. an understanding of risk exposure.

Answer: A

Explanation:

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

QUESTION NO: 329

Which of the following IT governance best practices improves strategic alignment?

A. Supplier and partner risks are managed.
B. A knowledge base on customers, products, markets and processes is in place.
C. A structure is provided that facilitates the creation and sharing of business information.
D. Top management mediate between the imperatives of business and technology.

Answer: D

Explanation:

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets andprocesses being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

QUESTION NO: 330

Effective IT governance requires organizational structures and processes to ensure that:

A. the organization's strategies and objectives extend the IT strategy.
B. the business strategy is derived from an IT strategy.
C. IT governance is separate and distinct from the overall governance.
D. the IT strategy extends the organization's strategies and objectives.

Answer: D

Explanation:

Effective IT governance requires that board and executive management extend governance to IT and provide the leadership, organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategiesand objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline;

it must become anintegral part of the overall enterprise governance.

QUESTION NO: 331

Which of the following is the MOST important element for the successful implementation of IT governance?

A. Implementing an IT scorecard
B. Identifying organizational strategies
C. Performing a risk assessment
D. Creating a formal security policy

Answer: B
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 NO: 332

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

A. IT budget.
B. existing IT environment.
C. business plan.
D. investment plan.

Answer: C
Explanation:
One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with thebusiness 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 NO: 333

When implementing an IT governance framework in an organization the MOST important objective is:

A. IT alignment with the business.

B. accountability.
C. value realization with IT.
D. enhancing the return on IT investments.

Answer: A
Explanation:
The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business {choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

QUESTION NO: 334

The ultimate purpose of IT governance is to:

A. encourage optimal use of IT.
B. reduce IT costs.
C. decentralize IT resources across the organization.
D. centralize control of IT.

Answer: A
Explanation:
IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

QUESTION NO: 335

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

A. Repeatable but Intuitive
B. Defined
C. Managed and Measurable
D. Optimized

Answer: B
Explanation:
Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

QUESTION NO: 336

Responsibility for the governance of IT should rest with the:

A. IT strategy committee.
B. chief information officer (CIO).
C. audit committee.
D. board of directors.

Answer: D
Explanation:
Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

QUESTION NO: 337

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?

A. User acceptance testing (UAT) occur for all reports before release into production
B. Organizational data governance practices be put in place
C. Standard software tools be used for report development
D. Management sign-off on requirements for new reports

Answer: B
Explanation:
This choice directly addresses the problem. An organizationwide 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 otherchoices, while sound development practices, do not address the root cause of the problem described.

QUESTION NO: 338

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

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

Answer: D

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 NO: 339

Which of the following would BEST provide assurance of the integrity of new staff?

A. Background screening
B. References
C. Bonding
D. Qualifications listed on a resume

Answer: A

Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligencecompliance, not at integrity, and qualifications listed on a resume may not be accurate.

QUESTION NO: 340

When an employee is terminated from service, the MOST important action is to:

A. hand over all of the employee's files to another designated employee.
B. complete a backup of the employee's work.
C. notify other employees of the termination.
D. disable the employee's logical access.

Answer: D

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

QUESTION NO: 341

Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivity.
B. reduce the opportunity for an employee to commit an improper or illegal act.
C. provide proper cross-training for another employee.
D. eliminate the potential disruption caused when an employee takes vacation one day at a time.

Answer: B
Explanation:
Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

QUESTION NO: 342

A local area network (LAN) administrator normally would be restricted from:

A. having end-user responsibilities.
B. reporting to the end-user manager.
C. having programming responsibilities.
D. being responsible for LAN security administration.

Answer: C
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 NO: 343

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

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

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

QUESTION NO: 344

An IS auditor should be concerned when a telecommunication analyst:

A. monitors systems performance and tracks problems resulting from program changes.
B. reviews network load requirements in terms of current and future transaction volumes.
C. assesses the impact of the network load on terminal response times and network data transfer rates.
D. recommends network balancing procedures and improvements.

Answer: A
Explanation:
The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes {choice B), assessing the impact of network load or terminal response times and network data transferrates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes {choice A) would put the analyst in a self-monitoring role.

QUESTION NO: 345

When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs

C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity

Answer: B
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 ITstaff 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 NO: 346

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single person.
B. inadequate succession planning.
C. one person knowing all parts of a system.
D. a disruption of operations.

Answer: C
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 NO: 347

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

A. Overlapping controls
B. Boundary controls
C. Access controls
D. Compensating controls

Answer: D

Explanation:

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

QUESTION NO: 348

Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives

Answer: C

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 NO: 349

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A. Deleting database activity logs
B. Implementing database optimization tools
C. Monitoring database usage
D. Defining backup and recovery procedures

Answer: A

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 NO: 350

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:

A. enterprise data model.
B. IT balanced scorecard (BSC).
C. IT organizational structure.
D. historical financial statements.

Answer: B
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 abilityto 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 NO: 351

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

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

Answer: B
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 NO: 352

Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

Answer: C
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 NO: 353

Which of the following is normally a responsibility of the chief security officer (CSO)?

A. Periodically reviewing and evaluating the security policy
B. Executing user application and software testing and evaluation
C. Granting and revoking user access to IT resources
D. Approving access to data and applications

Answer: A
Explanation:
The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

QUESTION NO: 354

To support an organization's goals, an IS department should have:

A. a low-cost philosophy.
B. long- and short-range plans.
C. leading-edge technology.
D. plans to acquire new hardware and software.

Answer: B

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 NO: 355

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

A. there is an integration of IS and business staffs within projects.
B. there is a clear definition of the IS mission and vision.
C. a strategic information technology planning methodology is in place.
D. the plan correlates business objectives to IS goals and objectives.

Answer: A

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 NO: 356

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs

Answer: A

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

QUESTION NO: 357

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

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

Answer: D
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 andwould thus be a part of the organization's strategic plan. The other choices are project-oriented and do not address business objectives.

QUESTION NO: 358

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line management.
B. does not vary from the IS department's preliminary budget.
C. complies with procurement procedures.
D. supports the business objectives of the organization.

Answer: D
Explanation:
Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrectsince line management prepared the plans.

QUESTION NO: 359

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environment.
B. the business plan.
C. the present IT budget.
D. current technology trends.

Answer: B

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 NO: 360

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

A. has all the personnel and equipment it needs.
B. plans are consistent with management strategy.
C. uses its equipment and personnel efficiently and effectively.
D. has sufficient excess capacity to respond to changing directions.

Answer: B

Explanation:

Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

QUESTION NO: 361

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?

A. Optimized
B. Managed
C. Defined
D. Repeatable

Answer: B

Explanation:

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

QUESTION NO: 362

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

A. control self-assessments.
B. a business impact analysis.
C. an IT balanced scorecard.
D. business process reengineering.

Answer: C
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 NO: 363

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

A. incorporates state of the art technology.
B. addresses the required operational controls.
C. articulates the IT mission and vision.
D. specifies project management practices.

Answer: C
Explanation:
The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

QUESTION NO: 364

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

A. establishment of a review board.
B. creation of a security unit.
C. effective support of an executive sponsor.
D. selection of a security process owner.

Answer: C
Explanation:
The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities.

Therefore, support by the executive level of management is themost critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

QUESTION NO: 365

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

A. an assessment of the fit of the organization's application portfolio with business objectives.
B. actions to reduce hardware procurement cost.
C. a listing of approved suppliers of IT contract resources.
D. a description of the technical architecture for the organization's network perimeter security.

Answer: A
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 toset 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 NO: 366

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

A. are developed for the organization as a whole.
B. are more likely to be derived as a result of a risk assessment.
C. will not conflict with overall corporate policy.
D. ensure consistency across the organization.

Answer: B
Explanation:
A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency

across the organization.

QUESTION NO: 367

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exist.
B. Specific user accountability cannot be established.
C. Unauthorized users may have access to originate, modify or delete data.
D. Audit recommendations may not be implemented.

Answer: C
Explanation:
Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

QUESTION NO: 368

The PRIMARY objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staff.
B. security and control policies support business and IT objectives.
C. there is a published organizational chart with functional descriptions.
D. duties are appropriately segregated.

Answer: B
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 NO: 369

The rate of change in technology increases the importance of:

A. outsourcing the IS function.

B. implementing and enforcing good processes.
C. hiring personnel willing to make a career within the organization.
D. meeting user requirements.

Answer: B
Explanation:
Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

QUESTION NO: 370

An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

A. this lack of knowledge may lead to unintentional disclosure of sensitive information.
B. information security is not critical to all functions.
C. IS audit should provide security training to the employees.
D. the audit finding will cause management to provide continuous training to staff.

Answer: A
Explanation:
All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

QUESTION NO: 371

The development of an IS security policy is ultimately the responsibility of the:

A. IS department.
B. security committee.
C. security administrator.
D. board of directors.

Answer: D
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 NO: 372

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

A. Response
B. Correction
C. Detection
D. Monitoring

Answer: A
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 NO: 373

Which of the following should be included in an organization's IS security policy?

A. A list of key IT resources to be secured
B. The basis for access authorization
C. Identity of sensitive security features
D. Relevant software security features

Answer: B
Explanation:
The security policy provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

QUESTION NO: 374

Which of the following is the initial step in creating a firewall policy?

A. A cost-benefit analysis of methods for securing the applications
B. Identification of network applications to be externally accessed
C. Identification of vulnerabilities associated with network applications to be externally accessed
D. Creation of an applications traffic matrix showing protection methods

Answer: B

Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

QUESTION NO: 375

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?

A. Utilization of an intrusion detection system to report incidents
B. Mandating the use of passwords to access all software
C. Installing an efficient user log system to track the actions of each user
D. Training provided on a regular basis to all current and new employees

Answer: D

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 NO: 376

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

A. Assimilation of the framework and intent of a written security policy by all appropriate parties
B. Management support and approval for the implementation and maintenance of a security policy
C. Enforcement of security rules by providing punitive actions for any violation of security rules
D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Answer: A

Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education onthe importance of security.

QUESTION NO: 377

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recovery.
B. retention.
C. rebuilding.
D. reuse.

Answer: B
Explanation:
Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the officialform of classic 'paper* makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

QUESTION NO: 378

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

A. implementation.
B. compliance.
C. documentation.
D. sufficiency.

Answer: D
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 NO: 379

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

A. the IT infrastructure.
B. organizational policies, standards and procedures.
C. legal and regulatory requirements.
D. the adherence to organizational policies, standards and procedures.

Answer: C
Explanation:
To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

QUESTION NO: 380

A top-down approach to the development of operational policies will help ensure:

A. that they are consistent across the organization.
B. that they are implemented as a part of risk assessment.
C. compliance with all policies.
D. that they are reviewed periodically.

Answer: A
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 NO: 381

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

A. Time zone differences could impede communications between IT teams.
B. Telecommunications cost could be much higher in the first year.
C. Privacy laws could prevent cross-border flow of information.
D. Software development may require more detailed specifications.

Answer: C
Explanation:
Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

QUESTION NO: 382

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?

A. Issues of privacy
B. Wavelength can be absorbed by the human body
C. RFID tags may not be removable
D. RFID eliminates line-of-sight reading

Answer: A
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 NO: 383

When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures
B. Defining a security policy
C. Specifying an access control methodology
D. Defining roles and responsibilities

Answer: B
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 willoften set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

QUESTION NO: 384

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:

A. report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
B. verify that user access rights have been granted on a need-to-have basis.
C. recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
D. recommend that activity logs of terminated users be reviewed on a regular basis.

Answer: C
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 NO: 385

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:

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

Answer: B
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, itmay 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.

QUESTION NO: 386

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

A. desired result or purpose of implementing specific control procedures.
B. best IT security control practices relevant to a specific entity.
C. techniques for securing information.
D. security policy.

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

QUESTION NO: 387

The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manual.
B. performance of a comprehensive security control review by the IS auditor.
C. adoption of a corporate information security policy statement.
D. purchase of security access control software.

Answer: C
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 NO: 388

Which of the following provides the best evidence of the adequacy of a security awareness program?

A. The number of stakeholders including employees trained at various levels

B. Coverage of training at all locations across the enterprise
C. The implementation of security devices from different vendors
D. Periodic reviews and comparison with best practices

Answer: D
Explanation:
The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

QUESTION NO: 389

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

A. provide strategic direction.
B. control business operations.
C. align IT with business.
D. implement best practices.

Answer: A
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 NO: 390

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

A. Define a balanced scorecard (BSC) for measuring performance
B. Consider user satisfaction in the key performance indicators (KPIs)
C. Select projects according to business benefits and risks
D. Modify the yearly process of defining the project portfolio

Answer: C
Explanation:
Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the

situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

QUESTION NO: 391

An example of a direct benefit to be derived from a proposed IT-related business investment is:

A. enhanced reputation.
B. enhanced staff morale.
C. the use of new technology.
D. increased market penetration.

Answer: D
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 NO: 392

To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

A. project management tools.
B. an object-oriented architecture.
C. tactical planning.
D. enterprise architecture (EA).

Answer: D
Explanation:
Enterprise architecture (EA) involves documenting the organization's IT assets and processes in a structured manner to facilitate understanding, management and planning for IT investments. It involves both a current state and a representation of an optimized future state. In attempting to complete an EA, organizations can address the problem either from a technology perspective or a business process perspective. Project management does not consider IT investment aspects; it is

a tool to aid in delivering projects. Object-oriented architecture is a software development methodology and does not assist in planning for IT investment, while tactical planning is relevant only after high-level IT investment decisions have been made.

QUESTION NO: 393

A benefit of open system architecture is that it:

A. facilitates interoperability.
B. facilitates the integration of proprietary components.
C. will be a basis for volume discounts from equipment vendors.
D. allows for the achievement of more economies of scale for equipment.

Answer: A
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 NO: 394

In the context of effective information security governance, the primary objective of value delivery is to:

A. optimize security investments in support of business objectives.
B. implement a standard set of security practices.
C. institute a standards-based solution.
D. implement a continuous improvement culture.

Answer: A
Explanation:
In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

QUESTION NO: 395

Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment (CSA)
B. Information systems audit
C. Investment portfolio analysis
D. Business risk assessment

Answer: C
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. Businessrisk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

QUESTION NO: 396

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?

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

Answer: B
Explanation:
The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger 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 postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralizedependencies 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 asorganizations and processes change to leverage the

intended synergy effects of the merger.

QUESTION NO: 397

Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees
D. Monitoring the outsourcing provider's performance

Answer: D
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 NO: 398

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

A. Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan.
B. Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract.
C. No, because the backup to be provided should be specified adequately in the contract.
D. No, because the service bureau's business continuity plan is proprietary information.

Answer: A
Explanation:
The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

QUESTION NO: 399

An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

A. hardware configuration.
B. access control software.
C. ownership of intellectual property.
D. application development methodology.

Answer: C
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 ofno 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 NO: 400

When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question regarding the legal jurisdiction.
B. Having a provider abroad will cause excessive costs in future audits.
C. The auditing process will be difficult because of the distance.
D. There could be different auditing norms.

Answer: A
Explanation:
In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

QUESTION NO: 401

An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

A. References from other customers
B. Service level agreement (SLA) template
C. Maintenance agreement
D. Conversion plan

Answer: A

Explanation:

An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows-issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

QUESTION NO: 402

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

A. O/S and hardware refresh frequencies
B. Gain-sharing performance bonuses
C. Penalties for noncompliance
D. Charges tied to variable cost metrics

Answer: B

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 NO: 403

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

A. Accountability for the corporate security policy
B. Defining the corporate security policy
C. Implementing the corporate security policy
D. Defining security procedures and guidelines

Answer: A

Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

QUESTION NO: 404

An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

A. That an audit clause is present in all contracts
B. That the SLA of each contract is substantiated by appropriate KPIs
C. That the contractual warranties of the providers support the business needs of the organization
D. That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Answer: C
Explanation:
The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

QUESTION NO: 405

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

A. Outsourced activities are core and provide a differentiated advantage to the organization.
B. Periodic renegotiation is specified in the outsourcing contract.
C. The outsourcing contract fails to cover every action required by the arrangement.
D. Similar activities are outsourced to more than one vendor.

Answer: A
Explanation:
An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, while multisourcing is an acceptable way to reduce risk.

QUESTION NO: 406

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 shouldbe that the:

A. requirement for protecting confidentiality of information could be compromised.
B. contract may be terminated because prior permission from the outsourcer was not obtained.
C. other service provider to whom work has been outsourced is not subject to audit.
D. outsourcer will approach the other service provider directly for further work.

Answer: A
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 not related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

QUESTION NO: 407

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?

A. Security incident summaries
B. Vendor best practices
C. CERT coordination center
D. Significant contracts

Answer: D
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 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 NO: 408

An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

A. documentation of staff background checks.
B. independent audit reports or full audit access.
C. reporting the year-to-year incremental cost reductions.
D. reporting staff turnover, development or training.

Answer: B

Explanation:

When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

QUESTION NO: 409

Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. meets or exceeds industry security standards.
B. agrees to be subject to external security reviews.
C. has a good market reputation for service and experience.
D. complies with security policies of the organization.

Answer: B

Explanation:

It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify orprove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

QUESTION NO: 410

The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

A. destruction policy.
B. security policy.
C. archive policy.
D. audit policy.

Answer: C

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 NO: 411

The output of the risk management process is an input for making:

A. business plans.
B. audit charters.
C. security policy decisions.
D. software design decisions.

Answer: C

Explanation:

The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

QUESTION NO: 412

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?

A. Report the risks to the CIO and CEO immediately
B. Examine e-business application in development
C. Identify threats and likelihood of occurrence
D. Check the budget available for risk management

Answer: C

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

QUESTION NO: 413

Which of the following is a mechanism for mitigating risks?

A. Security and control practices

B. Property and liability insurance
C. Audit and certification
D. Contracts and service level agreements (SLAs)

Answer: A

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 NO: 414

When developing a risk management program, what is the FIRST activity to be performed?

A. Threat assessment
B. Classification of data
C. Inventory of assets
D. Criticality analysis

Answer: C

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.

QUESTION NO: 415

A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

A. compute the amortization of the related assets.
B. calculate a return on investment (ROI).
C. apply a qualitative approach.
D. spend the time needed to define exactly the loss amount.

Answer: C

Explanation:

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor {e.g., one is a very low impact to thebusiness and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

QUESTION NO: 416

Which of the following does a lack of adequate security controls represent?

A. Threat
B. Asset
C. Impact
D. Vulnerability

Answer: D
Explanation:
The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to theloss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionalityin this context is a vulnerability.

QUESTION NO: 417

Assessing IT risks is BEST achieved by:

A. evaluating threats associated with existing IT assets and IT projects.
B. using the firm's past actual loss experience to determine current exposure.
C. reviewing published loss statistics from comparable organizations.
D. reviewing IT control weaknesses identified in audit reports.

Answer: A
Explanation:
To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient.Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to beassessed. 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 NO: 418

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:

A. avoidance.
B. transference.
C. mitigation.
D. acceptance.

Answer: C
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 NO: 419

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

A. vulnerabilities.
B. threats.
C. probabilities.
D. impacts.

Answer: A
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 NO: 420

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

A. identify the reasonable threats to the information assets.
B. analyze the technical and organizational vulnerabilities.
C. identify and rank the information assets.
D. evaluate the effect of a potential security breach.

Answer: C
Explanation:
Identification and ranking of information assets-e.g., data criticality, locations of assets-will set the tone or scope of how to assess risk in relation to the organizational value of the asset. Second, the threats facing each of the organization's assets should be analyzed according to their value to the organization. Third, weaknesses should be identified so that controls can be evaluated to determine if they mitigate the weaknesses. Fourth, analyze how these weaknesses, in absence of given controls, would impact the organization information assets.

QUESTION NO: 421

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

A. address all of the network risks.
B. be tracked over time against the IT strategic plan.
C. take into account the entire IT environment.
D. result in the identification of vulnerability tolerances.

Answer: C
Explanation:
When assessing IT security risk, it is important to take into account the entire IT environment. Measures of security risk should focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost. IT strategic plans are not granular enough to provide appropriate measures. Objective metrics must be tracked over time against measurable goals, thus the management of risk is enhanced by comparing today's results against last week, last month, last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk. They do not identify tolerances.

QUESTION NO: 422

Which of the following should be considered FIRST when implementing a risk management program?

A. An understanding of the organization's threat, vulnerability and risk profile
B. An understanding of the risk exposures and the potential consequences of compromise
C. A determination of risk management priorities based on potential consequences
D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Answer: A

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 NO: 423

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

A. performance measurement.
B. strategic alignment.
C. value delivery.
D. resource management.

Answer: A

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. 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 NO: 424

Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

A. Process maturity
B. Performance indicators
C. Business risk
D. Assurance reports

Answer: C

Explanation:

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

QUESTION NO: 425

The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

A. alignment of the IT activities with IS audit recommendations.
B. enforcement of the management of security risks.
C. implementation of the chief information security officer's (CISO) recommendations.
D. reduction of the cost for IT security.

Answer: B

Explanation:

The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risks. Recommendations, visions and objectives of the auditor and the chief information security officer (CISO) are usually included within a security program, but they would not be the major benefit. The cost of IT security may or may not be reduced.

QUESTION NO: 426

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?

A. Stricter controls should be implemented by both the organization and the cleaning agency.
B. No action is required since such incidents have not occurred in the past.
C. A clear desk policy should be implemented and strictly enforced in the organization.
D. A sound backup policy for all important office documents should be implemented.

Answer: A

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 NO: 427

During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management experts.
B. Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handle.
C. No recommendation is necessary since the current approach is appropriate for a medium-sized organization.
D. Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk management.

Answer: D
Explanation:
Establishing regular meetings is the best way to identify and assess risks in a medium-sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organizationwould normally not have a separate IT risk management department. Moreover, the risks are usually manageable enough so that external help would not be needed. While common risks may be covered by common industry standards, they cannot address the specific situation of an organization. Individual risks will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

QUESTION NO: 428

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

A. financial results.
B. customer satisfaction.
C. internal process efficiency.
D. innovation capacity.

Answer: A

Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

QUESTION NO: 429

Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient services.
B. define key performance indicators.
C. provide business value to IT projects.
D. control IT expenses.

Answer: B

Explanation:

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

QUESTION NO: 430

Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors
B. Gather performance data
C. Establish performance baselines
D. Optimize performance

Answer: D

Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

Topic 4, SYSTEMS AND INFRASTRUCTURE LIFECYCLE MANAGEMENT (130 PRACTICE

QUESTIONS)

QUESTION NO: 431

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

A. a clear business case has been approved by management.
B. corporate security standards will be met.
C. users will be involved in the implementation plan.
D. the new system will meet all required user functionality.

Answer: A
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 ofthe 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.

QUESTION NO: 432

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

A. the end of the system's life cycle.
B. the project is approved.
C. user acceptance of the system.
D. the system is in production.

Answer: A
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 dowe 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 shouldalways 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

QUESTION NO: 433

Which of the following risks could result from inadequate software baselining?

A. Scope creep
B. Sign-off delays
C. Software integrity violations
D. inadequate controls

Answer: A
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 businesscost-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. ChoicesB, C and D may not always result, but choice A is inevitable.

QUESTION NO: 434

The most common reason for the failure of information systems to meet the needs of users is that:

A. user needs are constantly changing.
B. the growth of user requirements was forecast inaccurately.
C. the hardware system limits the number of concurrent users.
D. user participation in defining the system's requirements was inadequate.

Answer: D
Explanation:
Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are, and therefore what the system should accomplish.

QUESTION NO: 435

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?

A. Function point analysis
B. PERT chart
C. Rapid application development
D. Object-oriented system development

Answer: B
Explanation:
A PERT chart will help determine project duration once all the activities and the work involved with

those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

QUESTION NO: 436

The reason for establishing a stop or freezing point on the design of a new system is to:

A. prevent further changes to a project in process.
B. indicate the point at which the design is to be completed.
C. require that changes after that point be evaluated for cost-effectiveness.
D. provide the project management team with more control over the project design.

Answer: C
Explanation:
Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.

QUESTION NO: 437

Change control for business application systems being developed using prototyping could be complicated by the:

A. iterative nature of prototyping.
B. rapid pace of modifications in requirements and design.
C. emphasis on reports and screens.
D. lack of integrated tools.

Answer: B
Explanation:
Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

QUESTION NO: 438

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?

A. Program evaluation review technique (PERT)
B. Counting source lines of code (SLOC)
C. Function point analysis
D. White box testing

Answer: C
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 techniquethat helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

QUESTION NO: 439

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

A. The project budget
B. The critical path for the project
C. The length of the remaining tasks
D. The personnel assigned to other tasks

Answer: B
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 NO: 440

Which of the following is a characteristic of timebox management?

A. Not suitable for prototyping or rapid application development (RAD)
B. Eliminates the need for a quality process
C. Prevents cost overruns and delivery delays
D. Separates system and user acceptance testing

Answer: C
Explanation:
Timebox management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

QUESTION NO: 441

Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

A. Project database
B. Policy documents
C. Project portfolio database
D. Program organization

Answer: C
Explanation:
A project portfolio database is the basis for project portfolio management. It includes project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. A project database may contain the above for one specific project and updates to various parameters pertaining to the current status of that single project. Policy documents on project management set direction for the design, development, implementation and monitoring of the project. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objective of the project.

QUESTION NO: 442

To minimize the cost of a software project, quality management techniques should be applied:

A. as close to their writing (i.e., point of origination) as possible.
B. primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
C. continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
D. mainly at project close-down to capture lessons learned that can be applied to future projects.

Answer: C

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 thatthe 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 NO: 443

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

A. whose sum of activity time is the shortest.
B. that have zero slack time.
C. that give the longest possible completion time.
D. whose sum of slack time is the shortest.

Answer: B

Explanation:

A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities onthe critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

QUESTION NO: 444

At the completion of a system development project, a postproject review should include which of the following?

A. Assessing risks that may lead to downtime after the production release
B. Identifying lessons learned that may be applicable to future projects
C. Verifying the controls in the delivered system are working

D. Ensuring that test data are deleted

Answer: B

Explanation:

A project team has something to learn from each and every project. As risk assessment is a key issue for project management, it is important for the organization to accumulate lessons learned and integrate them into future projects. An assessment ofpotential 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 postimplementation review. Test data should be retained for future regression testing.

QUESTION NO: 445

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

A. complexity and risks associated with the project have been analyzed.
B. resources needed throughout the project have been determined.
C. project deliverables have been identified.
D. a contract for external parties involved in the project has been completed.

Answer: A

Explanation:

Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome. The other choices, while important during the course of the project, cannot be fully determined at the time the project is initiated, and are often contingent upon the risk and complexity of the project.

QUESTION NO: 446

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 impactingthe project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
B. accept the project manager's position as the project manager is accountable for the outcome of the project.
C. offer to work with the risk manager when one is appointed.
D. 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.

Answer: A

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 these 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 ntpractices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

QUESTION NO: 447

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

A. effectiveness of the QA function because it should interact between project management and user management

B. efficiency of the QA function because it should interact with the project implementation team.

C. effectiveness of the project manager because the project manager should interact with the QA function.

D. efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Answer: A

Explanation:

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

QUESTION NO: 448

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

A. increases in quality can be achieved, even if resource allocation is decreased.
B. increases in quality are only achieved if resource allocation is increased.
C. decreases in delivery time can be achieved, even if resource allocation is decreased.
D. decreases in delivery time can only be achieved if quality is decreased.

Answer: A

Explanation:

The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

QUESTION NO: 449

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

A. Report that the organization does not have effective project management.
B. Recommend the project manager be changed.
C. Review the IT governance structure.
D. Review the conduct of the project and the business case.

Answer: D

Explanation:

Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound ITgovernance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

QUESTION NO: 450

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)?

A. Function point analysis
B. Earned value analysis
C. Cost budget
D. Program Evaluation and Review Technique

Answer: B

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 NO: 451

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

A. project be discontinued.
B. business case be updated and possible corrective actions be identified.
C. project be returned to the project sponsor for reapproval.
D. project be completed and the business case be updated later.

Answer: B

Explanation:

An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case. The IS auditor should recommend that the business case be kept current throughout the project since it is a key input to decisions made throughout the life of any project.

QUESTION NO: 452

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?

A. Project sponsor
B. System development project team (SPDT)
C. Project steering committee
D. User project team (UPT)

Answer: C

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 forthe 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.

QUESTION NO: 453

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor
B. Database administrator
C. Project manager
D. Data owner

Answer: D
Explanation:
During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted datA. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated datA. A project manager provides day-to-day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

QUESTION NO: 454

A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

A. what amount of progress against schedule has been achieved.

B. if the project budget can be reduced.
C. if the project could be brought in ahead of schedule.
D. if the budget savings can be applied to increase the project scope.

Answer: A
Explanation:
Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget after adjusting for actual progress, this is notnecessarily a good outcome because it points to flaws in the original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may be the wrong thing to do.

QUESTION NO: 455

A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

A. recommend that the project be halted until the issues are resolved.
B. recommend that compensating controls be implemented.
C. evaluate risks associated with the unresolved issues.
D. recommend that the project manager reallocate test resources to resolve the issues.

Answer: C
Explanation:
It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choicesmight be appropriate only after the risks have been assessed.

QUESTION NO: 456

Which of the following techniques would BEST help an IS auditor gain reasonable assurance that a project can meet its target date?

A. Estimation of the actual end date based on the completion percentages and estimated time to complete, taken from status reports
B. Confirmation of the target date based on interviews with experienced managers and staff involved in the completion of the project deliverables
C. Extrapolation of the overall end date based on completed work packages and current resources
D. Calculation of the expected end date based on current resources and remaining available project budget

Answer: C
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 fordependencies 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 NO: 457

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

A. Application programmers are implementing changes to production programs.
B. Application programmers are implementing changes to test programs.
C. Operations support staff are implementing changes to batch schedules.
D. Database administrators are implementing changes to data structures.

Answer: A
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 willaffect the scheduling of the batches only; it does not impact the live datA. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

QUESTION NO: 458

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

A. integrity.
B. authenticity.
C. authorization.
D. nonrepudiation.

Answer: A
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 beensured by using digital signatures.

QUESTION NO: 459

Before implementing controls, management should FIRST ensure that the controls:

A. satisfy a requirement in addressing a risk issue.
B. do not reduce productivity.
C. are based on a cost-benefit analysis.
D. are detective or corrective.

Answer: A
Explanation:
When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

QUESTION NO: 460

Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printout.
B. transaction journal.
C. automated suspense file listing.
D. user error report.

Answer: B
Explanation:
The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, while the user error report

would only list input that resulted in an edit error.

QUESTION NO: 461

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

A. Check digit
B. Existence check
C. Completeness check
D. Reasonableness check

Answer: C
Explanation:
A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteriA. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

QUESTION NO: 462

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

A. central processing site after running the application system.
B. central processing site during the running of the application system.
C. remote processing site after transmission of the data to the central processing site.
D. remote processing site prior to transmission of the data to the central processing site.

Answer: D
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 NO: 463

To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

A. during data preparation.
B. in transit to the computer.
C. between related computer runs.
D. during the return of the data to the user department.

Answer: A

Explanation:

During data preparation is the best answer, because it establishes control at the earliest point.

QUESTION NO: 464

Functional acknowledgements are used:

A. as an audit trail for EDI transactions.
B. to functionally describe the IS department.
C. to document user roles and responsibilities.
D. as a functional description of application software.

Answer: A

Explanation:

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

QUESTION NO: 465

A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

A. validation controls.
B. internal credibility checks.
C. clerical control procedures.
D. automated systems balancing.

Answer: D

Explanation:

Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checksare certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to summarize and compare inputs and outputs, an automated process is less susceptible to error.

QUESTION NO: 466

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

A. Test data/deck
B. Base-case system evaluation
C. Integrated test facility (ITF)
D. Parallel simulation

Answer: B
Explanation:
A base-case system evaluation uses test data sets developed as part of comprehensive testing programs, it is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

QUESTION NO: 467

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

A. Reasonableness check
B. Parity check
C. Redundancy check
D. Check digits

Answer: C
Explanation:
A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of datA. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the datA. A parity check isa hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

QUESTION NO: 468

Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check
B. Check digit
C. Validity check
D. Duplicate check

Answer: B

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered, e.g., an incorrect, but valid, value substituted for the original. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteriA. In a duplicate check, newor fresh transactions are matched to those previously entered to ensure that they are not already in the system.

QUESTION NO: 469

Which of the following is the GREATEST risk when implementing a data warehouse?

A. increased response time on the production systems
B. Access controls that are not adequate to prevent data modification
C. Data duplication
D. Data that is not updated or current

Answer: B

Explanation:

Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production datA. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

QUESTION NO: 470

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

A. Stringent contract management practices
B. Detailed and correctly applied specifications
C. Awareness of cultural and political differences
D. Postimplementation reviews

Answer: B

Explanation:

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

QUESTION NO: 471

Which of the following is the GREATEST risk to the effectiveness of application system controls?

A. Removal of manual processing steps
B. inadequate procedure manuals
C. Collusion between employees
D. Unresolved regulatory compliance issues

Answer: C
Explanation:
Collusion is an active attack that can be sustained and is difficult to identify since even well-thought-out application controls may be circumvented. The other choices do not impact well-designed application controls.

QUESTION NO: 472

The MAIN purpose of a transaction audit trail is to:

A. reduce the use of storage media.
B. determine accountability and responsibility for processed transactions.
C. help an IS auditor trace transactions.
D. provide useful information for capacity planning.

Answer: B
Explanation:
Enabling audit trails aids in establishing the accountability and responsibility for processed transactions by tracing them through the information system. Enabling audit trails increases the use of disk space. A transaction log file would be used totrace transactions, but would not aid in determining accountability and responsibility. The objective of capacity planning is the efficient and effective use of IT resources and requires information such as CPU utilization, bandwidth, number of users, etc.

QUESTION NO: 473

An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

A. acknowledge receipt of electronic orders with a confirmation message.

B. perform reasonableness checks on quantities ordered before filling orders.
C. verify the identity of senders and determine if orders correspond to contract terms.
D. encrypt electronic orders.

Answer: C
Explanation:
An electronic data interchange (EDI) system is subject not only to the usual risk exposures of computer systems but also to those arising from the potential ineffectiveness of controls on the part of the trading partner and the third-party service provider, making authentication of users and messages a major security concern. Acknowledging the receipt of electronic orders with a confirming message is good practice but will not authenticate orders from customers. Performing reasonableness checkson quantities ordered before placing orders is a control for ensuring the correctness of the company's orders, not the authenticity of its customers' orders. Encrypting sensitive messages is an appropriate step but does not apply to messages received.

QUESTION NO: 474

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
D. Reengineering the existing processing and redesigning the existing system

Answer: C
Explanation:
EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

QUESTION NO: 475

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

A. continuous improvement.

B. quantitative quality goals.
C. a documented process.
D. a process tailored to specific projects.

Answer: A

Explanation:

An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

QUESTION NO: 476

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

A. test the software for compatibility with existing hardware.
B. perform a gap analysis.
C. review the licensing policy.
D. ensure that the procedure had been approved.

Answer: D

Explanation:

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

QUESTION NO: 477

Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

A. System testing
B. Acceptance testing
C. Integration testing
D. Unit testing

Answer: B

Explanation:

Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level, as this could result in delays and cost overruns. System testing is undertaken by the developer team to determine if the software meets user requirements per specifications. Integration testing examines the units/modules as one integrated system and unit testing examines the individual units or components of the software. System, integration and unit testing are all performed by the developers at various stages of development; the impact of failure is comparatively less for each than failure at the acceptance testing stage.

QUESTION NO: 478

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?

A. Controls the proliferation of multiple versions of programs
B. Expands the programming resources and aids available
C. Increases program and processing integrity
D. Prevents valid changes from being overwritten by other changes

Answer: B
Explanation:
A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

QUESTION NO: 479

Which of the following is the most important element in the design of a data warehouse?

A. Quality of the metadata
B. Speed of the transactions
C. Volatility of the data
D. Vulnerability of the system

Answer: A
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 NO: 480
Ideally, stress testing should be carried out in a:

A. test environment using test data.
B. production environment using live workloads.
C. test environment using live workloads.
D. production environment using test data.

Answer: C
Explanation:
Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices Band D), and if only test data is used, there is no certainty that the system was stress tested adequately.

QUESTION NO: 481

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

A. inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism

Answer: C
Explanation:
Encapsulation is a property of objects, and it prevents accessing either properties or methods that have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.

QUESTION NO: 482

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Black box test
B. Desk checking
C. Structured walkthrough
D. Design and code

Answer: A
Explanation:
A black box test is a dynamic analysis tool for testing software modules. During the testing of software modules a black box test works first in a cohesive manner as a single unit/entity consisting of numerous modules, and second with the user data that flows across software

modules, in some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

QUESTION NO: 483

The phases and deliverables of a system development life cycle (SDLC) project should be determined:

A. during the initial planning stages of the project.
B. after early planning has been completed, but before work has begun.
C. throughout the work stages, based on risks and exposures.
D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate controls.

Answer: A
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 NO: 484

Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique

Answer: C
Explanation:
Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

QUESTION NO: 485

When implementing an application software package, which of the following presents the

GREATEST risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. incorrectly set parameters
D. Programming errors.

Answer: C
Explanation:
Parameters that are not set correctly would be the greatest concern when implementing an application software package. The other choices, though important, are a concern of the provider, not the organization that is implementing the software itself.

QUESTION NO: 486 CORRECT TEXT

Which of the following is an advantage of prototyping? A. The finished system normally has strong internal controls.

B. Prototype systems can provide significant time and cost savings.

C. Change control is often less complicated with prototype systems.

D. it ensures that functions or extras are not added to the intended system.

Answer: B
Explanation:
Prototype systems can provide significant time and cost savings; however, they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated, and it often leads to functions or extras being added to the system that were not originally intended.

QUESTION NO: 487

A decision support system (DSS):

A. is aimed at solving highly structured problems.
B. combines the use of models with nontraditional data access and retrieval functions.
C. emphasizes flexibility in the decision making approach of users.
D. supports only structured decision making tasks.

Answer: C
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 semistructureddecision making tasks.

QUESTION NO: 488

An advantage of using sanitized live transactions in test data is that:

A. all transaction types will be included.
B. every error condition is likely to be tested.
C. no special routines are required to assess the results.
D. test transactions are representative of live processing.

Answer: D
Explanation:
Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

QUESTION NO: 489

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:

A. users may prefer to use contrived data for testing.
B. unauthorized access to sensitive data may result.
C. error handling and credibility checks may not be fully proven.
D. the full functionality of the new process may not necessarily be tested.

Answer: B
Explanation:
Unless the data are sanitized, there is a risk of disclosing sensitive data.

QUESTION NO: 490

Which of the following is the PRIMARY purpose for conducting parallel testing?

A. To determine if the system is cost-effective
B. To enable comprehensive unit and system testing
C. To highlight errors in the program interfaces with files
D. To ensure the new system meets user requirements

Answer: D
Explanation:
The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements. Parallel testing may show that the old system is, in fact, better than the new system,

but this is not the primary reason. Unit and system testing are completed before parallel testing. Program interfaces with files are tested for errors during system testing.

QUESTION NO: 491

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:

A. rules.
B. decision trees.
C. semantic nets.
D. dataflow diagrams.

Answer: B
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 NO: 492

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

A. interface errors are detected earlier.
B. confidence in the system is achieved earlier.
C. errors in critical modules are detected earlier.
D. major functions and processing are tested earlier.

Answer: C
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.

QUESTION NO: 493

During which of the following phases in system development would user acceptance test plans normally be prepared?

A. Feasibility study
B. Requirements definition
C. implementation planning
D. Postimplementation review

Answer: B
Explanation:
During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document how the system functionality canbe tested to ensure it meets their stated needs. The feasibility study is too early for such detailed user involvement, and the implementation planning and postimplementation review phases are too late. An IS auditor should know at what point user testing should be planned to ensure it is most effective and efficient.

QUESTION NO: 494

The use of object-oriented design and development techniques would MOST likely:

A. facilitate the ability to reuse modules.
B. improve system performance.
C. enhance control effectiveness.
D. speed up the system development life cycle.

Answer: A
Explanation:
One of the major benefits of object-oriented design and development is the ability to reuse modules. The other options do not normally benefit from the object-oriented technique.

QUESTION NO: 495

Which of the following should be included in a feasibility study for a project to implement an EDI process?

A. The encryption algorithm format
B. The detailed internal control procedures
C. The necessary communication protocols
D. The proposed trusted third-party agreement

Answer: C
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 besignificant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.

QUESTION NO: 496

When a new system is to be implemented within a short time frame, it is MOST important to:

A. finish writing user manuals.
B. perform user acceptance testing.
C. add last-minute enhancements to functionalities.
D. ensure that the code has been documented and reviewed.

Answer: B
Explanation:
It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirements.

QUESTION NO: 497

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. a backup server be available to run ETCS operations with up-to-date data.
B. a backup server be loaded with all the relevant software and data.
C. the systems staff of the organization be trained to handle any event.
D. source code of the ETCS application be placed in escrow.

Answer: D
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 NO: 498

The MOST likely explanation for the use of applets in an Internet application is that:

A. it is sent over the network from the server.
B. the server does not run the program and the output is not sent over the network.
C. they improve the performance of the web server and network.
D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Answer: C
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 NO: 499

A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing system developed in-house. in reviewing the proposed development approach, which of the following would be of GREATESTconcern?

A. Acceptance testing is to be managed by users.
B. A quality plan is not part of the contracted deliverables.
C. Not all business functions will be available on initial implementation.
D. Prototyping is being used to confirm that the system meets business requirements.

Answer: B
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 NO: 500

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?

A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers

Answer: B

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 NO: 501

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:

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

Answer: A

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 andchoice D refers to efficiency.

QUESTION NO: 502

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:

A. increased maintenance.
B. improper documentation of testing.
C. inadequate functional testing.
D. delays in problem resolution.

Answer: C

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 NO: 503

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

A. facilitates user involvement.
B. allows early testing of technical features.
C. facilitates conversion to the new system.
D. shortens the development time frame.

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

QUESTION NO: 504

An IS auditor reviewing a proposed application software acquisition should ensure that the:

A. operating system (OS) being used is compatible with the existing hardware platform.
B. planned OS updates have been scheduled to minimize negative impacts on company needs.
C. OS has the latest versions and updates.
D. products are compatible with the current or planned OS.

Answer: D
Explanation:
Choices A, B and C are incorrect because none of them are related to the area being audited. In reviewing the proposed application the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

QUESTION NO: 505

The GREATEST benefit in implementing an expert system is the:

A. capturing of the knowledge and experience of individuals in an organization.

B. sharing of knowledge in a central repository.
C. enhancement of personnel productivity and performance.
D. reduction of employee turnover in key departments.

Answer: A

Explanation:

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit; however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

QUESTION NO: 506

By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

A. reliable products are guaranteed.
B. programmers' efficiency is improved.
C. security requirements are designed.
D. predictable software processes are followed.

Answer: D

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 NO: 507

The waterfall life cycle model of software development is most appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
B. requirements are well understood and the project is subject to time pressures.
C. the project intends to apply an object-oriented design and programming approach.
D. the project will involve the use of new technology.

Answer: A

Explanation:

Historically, the waterfall model has been best suited to the stable conditions described in choice A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. Theability 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 NO: 508

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

A. A sufficient quantity of data for each test case
B. Data representing conditions that are expected in actual processing
C. Completing the test on schedule
D. A random sample of actual data

Answer: B
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 NO: 509

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:

A. buffer overflow.
B. brute force attack.
C. distributed denial-of-service attack.
D. war dialing attack.

Answer: A
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.

QUESTION NO: 510

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

A. Bottom up
B. Sociability testing
C. Top-down
D. System test

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

QUESTION NO: 511

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

A. test data covering critical applications.
B. detailed test plans.
C. quality assurance test specifications.
D. user acceptance testing specifications.

Answer: D
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 NO: 512
Which of the following is an advantage of the top-down approach to software testing?

A. Interface errors are identified early
B. Testing can be started before all programs are complete
C. it is more effective than other testing approaches
D. Errors in critical modules are detected sooner

Answer: A

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 areadvantages of the bottom-up approach to system testing.

QUESTION NO: 513

During the system testing phase of an application development project the IS auditor should review the:

A. conceptual design specifications.
B. vendor contract.
C. error reports.
D. program change requests.

Answer: C

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. Aconceptual 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 NO: 514

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

A. increase the time allocated for system testing
B. implement formal software inspections
C. increase the development staff
D. Require the sign-off of all project deliverables

Answer: B

Explanation:

Inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce. Deliverable reviews normally do not go down to the same level of detail as software inspections.

QUESTION NO: 515

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

A. Applications may not be subject to testing and IT general controls
B. increased development and maintenance costs
C. increased application development time
D. Decision-making may be impaired due to diminished responsiveness to requests for information

Answer: A
Explanation:
End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls,quality assurance procedures, and documentation. A risk of end-user applications is that management may rely on them as much as traditional applications. End-user computing (EUC) systems typically result in reduced application development and maintenance costs, and a reduced development cycle time. EUC systems normally increase flexibility and responsiveness to management's information requests.

QUESTION NO: 516

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

A. System owners
B. System users
C. System designers
D. System builders

Answer: A

Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system. Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

QUESTION NO: 517

The MAJOR advantage of a component-based development approach is the:

A. ability to manage an unrestricted variety of data types.
B. provision for modeling complex relationships.
C. capacity to meet the demands of a changing environment.
D. support of multiple development environments.

Answer: D

Explanation:

Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not themost significant advantages of a component-based development approach.

QUESTION NO: 518

The specific advantage of white box testing is that it:

A. verifies a program can operate successfully with other parts of the system.
B. ensures a program's functional operating effectiveness without regard to the internal program structure.
C. determines procedural accuracy or conditions of a program's specific logic paths.
D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Answer: C

Explanation:

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

QUESTION NO: 519

Following best practices, formal plans for implementation of new information systems are developed during the:

A. development phase.
B. design phase.
C. testing phase.
D. deployment phase.

Answer: B
Explanation:
Planning for implementation should begin well in advance of the actual implementation date. A formal implementation plan should be constructed in the design phase and revised as the development progresses.

QUESTION NO: 520

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?

A. Use of a process-based maturity model such as the capability maturity model (CMM)
B. Regular monitoring of task-level progress against schedule
C. Extensive use of software development tools to maximize team productivity
D. Postiteration reviews that identify lessons learned for future use in the project

Answer: D
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, atthe end of each iteration, the team considers and documents what worked well and what could have worked better, and identifies improvements to be implemented in subsequent iterations. CMM and Agile really sit at opposite poles. CMM places heavy emphasis on predefined formal processes and formal project management and software development deliverables. Agile projects, by contrast, rely on refinement of process as dictated by the particular needs of the project and team dynamics. Additionally, less importance is placed on formal paper-based deliverables, with the preference being effective informal communication within the team and with key outside contributors. Agile

projects produce releasable software in short iterations, typically ranging from 4 to 8 weeks. This, in itself, instills considerable performance discipline within the team. This, combined with short daily meetings to agree on what the team is doing and the identification of any impediments, renders task-level tracking against a schedule redundant. Agile projects do make use of suitable development tools; however, tools are not seen as the primary means of achieving productivity. Team harmony, effective communications and collective ability to solve challenges are of

QUESTION NO: 521

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?

A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day
C. implement a source code version control tool
D. Only retest high priority defects

Answer: A
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 migratedto production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

QUESTION NO: 522

Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing
B. Pilot testing

C. Interface/integration testing
D. Sociability testing

Answer: D
Explanation:
The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system-and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another.The objective is to take unit-tested modules and build an integrated structure.

QUESTION NO: 523

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

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

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

QUESTION NO: 524

Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. inability to specify purpose and usage patterns
D. Changes in decision processes

Answer: C

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 DSS.

QUESTION NO: 525

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

A. Pilot
B. Parallel
C. Direct cutover
D. Phased

Answer: C

Explanation:

Direct cutover implies switching to the new system immediately, usually without the ability to revert to the old system in the event of problems. All other alternatives are done gradually and thus provide greater recoverability and are therefore less risky.

QUESTION NO: 526

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

A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run

Answer: D

Explanation:

Parallel runs are the safest-though the most expensive-approach, because both the old and new systems are run, thus incurring what might appear to be double costs. Direct cutover is actually quite risky, since it does not provide for a 'shake down period' nor does it provide an easy fallback option. Both a pilot study and a phased approach are performedincrementally, making rollback procedures difficult to execute.

QUESTION NO: 527

Which of the following would impair the independence of a quality assurance team?

A. Ensuring compliance with development methods
B. Checking the testing assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation

Answer: C
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 NO: 528

From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

A. a big bang deployment after proof of concept.
B. prototyping and a one-phase deployment.
C. a deployment plan based on sequenced phases.
D. to simulate the new infrastructure before deployment.

Answer: C
Explanation:
When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

QUESTION NO: 529

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:

A. correlation of semantic characteristics of the data migrated between the two systems.
B. correlation of arithmetic characteristics of the data migrated between the two systems.
C. correlation of functional characteristics of the processes between the two systems.
D. relative efficiency of the processes between the two systems.

Answer: A
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 NO: 530

The reason a certification and accreditation process is performed on critical systems is to ensure that:

A. security compliance has been technically evaluated.
B. data have been encrypted and are ready to be stored.
C. the systems have been tested to run on different platforms.
D. the systems have followed the phases of a waterfall model.

Answer: A
Explanation:
Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

QUESTION NO: 531

During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

A. review access control configuration.
B. evaluate interface testing.
C. review detailed design documentation.
D. evaluate system testing.

Answer: A
Explanation:
Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system. Since a postimplementation review is done after user acceptance testing and actual implementation, onewould not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system, since these are usually vendor packages with user manuals. System testing should be performed before final user signoff.

QUESTION NO: 532

During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

A. implement data backup and recovery procedures.
B. Define standards and closely monitor for compliance.
C. Ensure that only authorized personnel can update the database.
D. Establish controls to handle concurrent access problems.

Answer: A
Explanation:
Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, while monitoring for compliance is adetective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

QUESTION NO: 533

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?

A. Log all table update transactions.
B. implement before-and-after image reporting.
C. Use tracing and tagging.
D. implement integrity constraints in the database.

Answer: D
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 NO: 534

Responsibility and reporting lines cannot always be established when auditing automated systems since:

A. diversified control makes ownership irrelevant.
B. staff traditionally changes jobs with greater frequency.
C. ownership is difficult to establish where resources are shared.
D. duties change frequently in the rapid development of technology.

Answer: C

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 NO: 535

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:

A. isolation.
B. consistency.
C. atomicity.
D. durability.

Answer: C

Explanation:

The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the databasebe 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 NO: 536

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

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

Answer: B

Explanation:

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

QUESTION NO: 537

Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

A. Develop a baseline and monitor system usage.
B. Define alternate processing procedures.
C. Prepare the maintenance manual.
D. implement the changes users have suggested.

Answer: A
Explanation:
An IS auditor should recommend the development of a performance baseline and monitor the system's performance, against the baseline, to develop empirical data upon which decisions for modifying the system can be made. Alternate processing proceduresand a maintenance manual will not alter a system's performance. Implementing changes without knowledge of thecause(s)forthe perceived poor performance may not result in a more efficient system.

QUESTION NO: 538

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?

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

Answer: A
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, butthey are not the auditor's primary concern.

QUESTION NO: 539

A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

Answer: A
Explanation:
Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processingcentrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

QUESTION NO: 540

When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

A. systems receiving the output of other systems.
B. systems sending output to other systems.
C. systems sending and receiving data.
D. interfaces between the two systems.

Answer: C
Explanation:
Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

QUESTION NO: 541

An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

A. EDI trading partner agreements.
B. physical controls for terminals.
C. authentication techniques for sending and receiving messages.
D. program change control procedures.

Answer: C

Explanation:

Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

QUESTION NO: 542

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:

A. check to ensure that the type of transaction is valid for the card type.
B. verify the format of the number entered then locate it on the database.
C. ensure that the transaction entered is within the cardholder's credit limit.
D. confirm that the card is not shown as lost or stolen on the master file.

Answer: B

Explanation:

The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed. A validation control in data capture will ensure that the data entered is valid (i.e., it can be processed by the system). If the data captured in the initial validation is not valid (if the card number or PIN do not match with the database), then the card will be rejected or captured per the controls in place. Once initial validation is completed, then other validations specific to the card and cardholder would be performed.

QUESTION NO: 543

A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification
B. One-for-one checking
C. Manual recalculations
D. Functional acknowledgements

Answer: D

Explanation:

Acting as an audit trail for EDI transactions, functional acknowledgements are one of the main controls used in data mapping. All the other choices are manual input controls, whereas data mapping deals with automatic integration of data in the receiving company.

QUESTION NO: 544

Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:

A. pre-BPR process flowcharts.
B. post-BPR process flowcharts.
C. BPR project plans.
D. continuous improvement and monitoring plans.

Answer: B
Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Choice A is incorrect because an IS auditor must review the process as it is today, not as it was in the past. Choices C and D areincorrect because they are steps within a BPR project.

QUESTION NO: 545

A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:

A. payroll reports should be compared to input forms.
B. gross payroll should be recalculated manually.
C. checks (cheques) should be compared to input forms.
D. checks (cheques) should be reconciled with output reports.

Answer: A
Explanation:
The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports. Hence, comparing payroll reports with input forms isthe best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques)have the processed information and input forms have the input datA. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

QUESTION NO: 546

Which of the following represents the GREATEST potential risk in an EDI environment?

A. Transaction authorization

B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A
Explanation:
Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

QUESTION NO: 547

Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

A. Accuracy of the source data
B. Credibility of the data source
C. Accuracy of the extraction process
D. Accuracy of the data transformation

Answer: A
Explanation:
Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source, accurate extraction processes and accurate transformation routines are all important, but would not change inaccurate data intoquality (accurate) data.

QUESTION NO: 548

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

A. Use of a cryptographic hashing algorithm
B. Enciphering the message digest
C. Deciphering the message digest
D. A sequence number and time stamp

Answer: D
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 toverify that a payment instruction

was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

QUESTION NO: 549

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. not be concerned since there may be other compensating controls to mitigate the risks.
B. ensure that overrides are automatically logged and subject to review.
C. verify whether all such overrides are referred to senior management for approval.
D. recommend that overrides not be permitted.

Answer: B
Explanation:
If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. Aslong as the overrides are policy-compliant, there is no need for senior management approval or a blanket prohibition.

QUESTION NO: 550

When using an integrated test facility (ITF), an IS auditor should ensure that:

A. production data are used for testing.
B. test data are isolated from production data.
C. a test data generator is used.
D. master files are updated with the test data.

Answer: B
Explanation:
An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live datA. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production datA. An IS auditor is not required to use production data or a test data generator. Production master files should not be updated with test data.

QUESTION NO: 551

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?

A. The system will not process the change until the clerk's manager confirms the change by entering an approval code.
B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager.
C. The system requires the clerk to enter an approval code.
D. The system displays a warning message to the clerk.

Answer: A
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. ChoicesC and D do not prevent the clerk from entering an unauthorized rate change.

QUESTION NO: 552

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

A. secure communications.
B. improved performance.
C. efficient interfacing.
D. enhanced documentation.

Answer: C
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 NO: 553

An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are inplace. The BEST response the auditor can make is to:

A. review the integrity of system access controls.

B. accept management's statement that effective access controls are in place.
C. stress the importance of having a system control framework in place.
D. review the background checks of the accounts payable staff.

Answer: C
Explanation:
Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

QUESTION NO: 554

When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

A. excessive transaction turnaround time.
B. application interface failure.
C. improper transaction authorization.
D. nonvalidated batch totals.

Answer: C
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 assignificant.

QUESTION NO: 555

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

A. The risks associated with the use of the products are periodically assessed
B. The latest version of software is listed for each product
C. Due to licensing issues the list does not contain open source software

D. After hours support is offered

Answer: A

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 andD are possible considerations but would not be the most important.

QUESTION NO: 556

An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineering.
B. prototyping.
C. software reuse.
D. reengineering.

Answer: D

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 NO: 557

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 performing adequately which of the following types of testing?

A. Unit testing
B. Integration testing
C. Design walkthroughs
D. Configuration management

Answer: B

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.

QUESTION NO: 558

An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. authorization of program changes.
B. creation date of a current object module.
C. number of program changes actually made.
D. creation date of a current source program.

Answer: A

Explanation:

The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

QUESTION NO: 559

After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

A. Stress
B. Black box
C. Interface
D. System

Answer: D

Explanation:

Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

QUESTION NO: 560

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?

A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
C. A single implementation is planned, immediately decommissioning the legacy system.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.

Answer: C
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 thecase, 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.

Topic 5, IT SERVICE DELIVERY AND SUPPORT (116 PRACTICE QUESTIONS)

QUESTION NO: 561

Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

Answer: D
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 NO: 562

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

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

Answer: C
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.

QUESTION NO: 563

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?

A. Overall number of users supported
B. Percentage of incidents solved in the first call
C. Number of incidents reported to the help desk
D. Number of agents answering the phones

Answer: B
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 NO: 564

The PRIMARY objective of service-level management (SLM) is to:

A. define, agree, record and manage the required levels of service.
B. ensure that services are managed to deliver the highest achievable level of availability.
C. keep the costs associated with any service at a minimum.
D. monitor and report any legal noncompliance to business management.

Answer: A
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 atthe highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level, since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

QUESTION NO: 565

Which of the following should be of PRIMARY concern to an IS auditor reviewing the

management of external IT service providers?

A. Minimizing costs for the services provided
B. Prohibiting the provider from subcontracting services
C. Evaluating the process for transferring knowledge to the IT department
D. Determining if the services were provided as contracted

Answer: D
Explanation:
From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department. Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

QUESTION NO: 566

IT best practices for the availability and continuity of IT services should:

A. minimize costs associated with disaster-resilient components.
B. provide for sufficient capacity to meet the agreed upon demands of the business.
C. provide reasonable assurance that agreed upon obligations to customers can be met.
D. produce timely performance metric reports.

Answer: C
Explanation:
It is important that negotiated and agreed commitments (i.e., service level agreements [SLAs]) can be fulfilled all the time. If this were not achievable, IT should not have agreed to these requirements, as entering into such a commitment would be misleading to the business. 'All the time' in this context 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 NO: 567

During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do FIRST?

A. Postpone the audit until the agreement is documented
B. Report the existence of the undocumented agreement to senior management
C. Confirm the content of the agreement with both departments
D. Draft a service level agreement (SLA) for the two departments

Answer: C
Explanation:
An IS auditor should first confirm and understand the current practice before making any recommendations. The agreement can be documented after it has been established that there is an agreement in place. The fact that there is not a written agreement does not justify postponing the audit, and reporting to senior management is not necessary at this stage of the audit. Drafting a service level agreement (SLA) is not the IS auditor's responsibility.

QUESTION NO: 568

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?

A. The use of diskless workstations
B. Periodic checking of hard drives
C. The use of current antivirus software
D. Policies that result in instant dismissal if violated

Answer: B
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. Disklessworkstations 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 NO: 569

To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files
B. Enabled access control software parameters
C. Logs of access control violations
D. System configuration files for control options used

Answer: D
Explanation:
A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

QUESTION NO: 570

Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?

A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log

D. A written preventive maintenance schedule

Answer: A

Explanation:

A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

QUESTION NO: 571

Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?

A. Sensitive data can be read by operators.
B. Data can be amended without authorization.
C. Unauthorized report copies can be printed.
D. Output can be lost in the event of system failure.

Answer: C

Explanation:

Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

QUESTION NO: 572

Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set.
B. data will not be deleted before that date.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.

Answer: B

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 NO: 573

Which of the following is a network diagnostic tool that monitors and records network information?

A. Online monitor
B. Downtime report
C. Help desk report
D. Protocol analyzer

Answer: D
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 NO: 574

Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite

Answer: B
Explanation:
A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

QUESTION NO: 575

IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
B. The service provider does not have incident handling procedures.
C. Recently a corrupted database could not be recovered because of library management problems.

D. incident logs are not being reviewed.

Answer: A

Explanation:

The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

QUESTION NO: 576

Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location
B. Setting a boot password
C. Hardening the server configuration
D. Implementing activity logging

Answer: C

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 accesscan modify logs or disable them.

QUESTION NO: 577

The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:

A. contents are highly volatile.
B. data cannot be backed up.
C. data can be copied.
D. device may not be compatible with other peripherals.

Answer: C

Explanation:

Unless properly controlled, flash memory provides an avenue for anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

QUESTION NO: 578

The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentiality.
B. increased redundancy.
C. unauthorized accesses.
D. application malfunctions.

Answer: B
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 NO: 579

Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

A. protect the organization from viruses and nonbusiness materials.
B. maximize employee performance.
C. safeguard the organization's image.
D. assist the organization in preventing legal issues

Answer: A
Explanation:
The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it wouldneed to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

QUESTION NO: 580

The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

A. compression software to minimize transmission duration.
B. functional or message acknowledgments.
C. a packet-filtering firewall to reroute messages.
D. leased asynchronous transfer mode lines.

Answer: D
Explanation:
Leased asynchronous transfer mode lines are a way to avoid using public and shared infrastructures from the carrier or Internet service provider that have a greater number of communication failures. Choice A, compression software, is a valid way to reduce the problem, but is not as good as leased asynchronous transfer mode lines. Choice B is a control based on higher protocol layers and helps if communication lines are introducing noise, but not if a link is down. Choice C, a packet-filtering firewall, does not reroute messages.

QUESTION NO: 581

An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

A. source documentation retention.
B. data file security.
C. version usage control.
D. one-for-one checking.

Answer: C
Explanation:
For processing to be correct, it is essential that the proper version of a file is used. Transactions should be applied to the most current database, while restart procedures should use earlier versions. Source documentation should be retained for anadequate time period to enable documentation retrieval, reconstruction or verification of data, but it does not aid in ensuring that the correct version of a file will be used. Data file security controls prevent access by unauthorized users who could then alter the data files; however, it does not ensure that the correct file will be used. It is necessary to ensure that all documents have been received for processing, one-for-one; however, this does not ensure the use of the correct file.

QUESTION NO: 582

Which of the following BEST limits the impact of server failures in a distributed environment?

A. Redundant pathways
B. Clustering
C. Dial backup lines
D. Standby power

Answer: B
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 NO: 583

When reviewing a hardware maintenance program, an IS auditor should assess whether:

A. the schedule of all unplanned maintenance is maintained.
B. it is in line with historical trends.
C. it has been approved by the IS steering committee.
D. the program is validated against vendor specifications.

Answer: D
Explanation:
Though maintenance requirements vary based on complexity and performance work loads, 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 NO: 584

An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

A. Staging and job set up
B. Supervisory review of logs
C. Regular back-up of tapes
D. Offsite storage of tapes

Answer: A

Explanation:

If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a compensating control. Choice B is a detective control while choices C and D are corrective controls, none of which would serve as good compensating controls.

QUESTION NO: 585

To verify that the correct version of a data file was used for a production run, an IS auditor should review:

A. operator problem reports.
B. operator work schedules.
C. system logs.
D. output distribution reports.

Answer: C
Explanation:

System logs are automated reports which identify most of the activities performed on the computer. Programs that analyze the system log have been developed to report on specifically defined items. The auditor can then carry out tests to ensure that the correct file version was used for a production run. Operator problem reports are used by operators to log computer operation problems. Operator work schedules are maintained to assist in human resources planning. Output distribution reports identify all application reports generated and their distribution.

QUESTION NO: 586

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. A security information event management (SIEM) product
B. An open-source correlation engine
C. A log management tool
D. An extract, transform, load (ETL) system

Answer: C
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 differentstatistics 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 correlatesevents 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 NO: 587

Doing which of the following during peak production hours could result in unexpected downtime?

A. Performing data migration or tape backup
B. Performing preventive maintenance on electrical systems
C. Promoting applications from development to the staging environment
D. Replacing a failed power supply in the core router of the data center

Answer: B
Explanation:
Choices A and C are processing events which may impact performance, but would not cause downtime. Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenanceactivities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

QUESTION NO: 588

Which of the following would BEST maintain the integrity of a firewall log?

A. Granting access to log information only to administrators
B. Capturing log events in the operating system layer
C. Writing dual logs onto separate storage media
D. Sending log information to a dedicated third-party log server

Answer: D
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. Thereare many ways to capture log information: through the application layer, network layer, operating systems layer, etc.; however, there is no log integrity advantage in capturing

events in the operating systems layer. If it is a highly mission-critical information system, it may be nice to run the system with a dual log mode. Having logs in two different storage devices will primarily contribute to the assurance of the availability of log information, rather than to maintaining its integrity.

QUESTION NO: 589

Which of the following will prevent dangling tuples in a database?

A. Cyclic integrity
B. Domain integrity
C. Relational integrity
D. Referential integrity

Answer: D
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., forexistence 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 sourcedocumentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

QUESTION NO: 590

The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized users.
B. prevent integrity problems when two processes attempt to update the same data at the same time.
C. prevent inadvertent or unauthorized disclosure of data in the database.
D. ensure the accuracy, completeness and consistency of data.

Answer: B
Explanation:
Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users, and controls such as passwords preventthe 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 NO: 591

Which of the following controls would provide the GREATEST assurance of database integrity?

A. Audit log procedures
B. Table link/reference checks
C. Query/table access time checks
D. Rollback and rollforward database features

Answer: B
Explanation:
Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database), and thus provides the greatest assurance of database integrity. Audit log procedures enable recording ofall events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database's contents. Querying/monitoring table access time checks helps designers improve database performance, but not integrity. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

QUESTION NO: 592

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?

A. Consistency
B. Isolation
C. Durability
D. Atomicity

Answer: D
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 NO: 593
During maintenance of a relational database, several values of the foreign key in a transaction

table of a relational database have been corrupted. The consequence is that:

A. the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
B. there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
C. the database will immediately stop execution and lose more information.
D. the database will no longer accept input data.

Answer: A
Explanation:
When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction datA. This will normally cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be unacceptable. Choice B is incorrect, since a system can recover the corrupted external key by reindexing the table. Choices C and D would not result from a corrupted foreignkey.

QUESTION NO: 594

In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

A. Foreign key
B. Primary key
C. Secondary key
D. Public key

Answer: A
Explanation:
In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database. It should not be possible to delete a row from acustomer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table, so it is not able to provide/ensure referential integrity by itself. Secondary keys that are not foreign keys are not subject to referential integrity checks. Public key is related to encryption and not linked in any way to referential integrity.

QUESTION NO: 595

When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

A. recommend that the database be normalized.
B. review the conceptual data model.
C. review the stored procedures.
D. review the justification.

Answer: D

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 NO: 596

A database administrator has detected a performance problem with some tables which

could be solved through denormalization. This situation will increase the risk of:

A. concurrent access.
B. deadlocks.
C. unauthorized access to data.
D. a loss of data integrity.

Answer: D

Explanation:

Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

QUESTION NO: 597

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?

A. increase the frequency for data replication between the different department systems to ensure timely updates.
B. Centralize all request processing in one department to avoid parallel processing of the same request.
C. Change the application architecture so that common data are held in just one shared database for all departments.

D. implement reconciliation controls to detect duplicates before orders are processed in the systems.

Answer: C

Explanation:

Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannotbe 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 NO: 598

Which of the following database controls would ensure that the integrity of transactions

is maintained in an online transaction processing system's database?

A. Authentication controls
B. Data normalization controls
C. Read/write access log controls
D. Commitment and rollback controls

Answer: D

Explanation:

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

QUESTION NO: 599

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?

A. Permanent table-space allocation
B. Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls

Answer: C

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 NO: 600

Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server troubleshooting

Answer: A

Explanation:

Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally, it also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server troubleshooting is used for troubleshooting purposes.

QUESTION NO: 601

Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

A. Parity check
B. Echo check
C. Block sum check
D. Cyclic redundancy check

Answer: D

Explanation:

The cyclic redundancy check (CRC) can check for a block of transmitted datA. The workstations generate the CRC and transmit it with the datA. The receiving workstation computes a CRC and compares it to the transmitted CRC. if both of them are equal.then the block is assumed error free, in this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. Inhigher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

QUESTION NO: 602

Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screening router
B. Packet filter
C. Application gateway
D. Circuit gateway

Answer: C

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 meansthat 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 programthat acts as an intermediary between external and internal accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy(which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

QUESTION NO: 603

Which of the following is MOST directly affected by network performance monitoring tools?

A. Integrity

B. Availability
C. Completeness
D. Confidentiality

Answer: B
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 NO: 604

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:

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

Answer: A
Explanation:
The peak at 96 percent could be the result of a one-off incident, e.g., a user downloading a large amount of data; therefore, analysis to establish whether this is a regular pattern and what causes this behavior should be carried out before expenditure on a larger line capacity is recommended. Since the link provides for a standby database, a short loss of this service should be acceptable. If the peak is established to be a regular occurrence without any other opportunities for mitigation (usage of bandwidth reservation protocol, or other types of prioritizing network traffic), the line should be replaced as there is the risk of loss of service as the traffic approaches 100 percent. If, however, the peak is a one-off or can be put in othertime frames, then user education may be an option.

QUESTION NO: 605

While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

A. recommend the use of disk mirroring.
B. review the adequacy of offsite storage.
C. review the capacity management process.
D. recommend the use of a compression algorithm.

Answer: C
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 NO: 606

In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

Answer: C
Explanation:
While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

QUESTION NO: 607

Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

A. Assess the impact of patches prior to installation.
B. Ask the vendors for a new software version with all fixes included.
C. install the security patch immediately.
D. Decline to deal with these vendors in the future.

Answer: A

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 withall fixes included are not always available and a full installation could be time consuming. Declining to deal with vendors does not take care of the flaw.

QUESTION NO: 608

Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports
B. Library control software restricting changes to source code
C. Restricted access to source code and object code
D. Date and time-stamp reviews of source and object code

Answer: D

Explanation:

Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is theone being used.

QUESTION NO: 609

Change management procedures are established by IS management to:

A. control the movement of applications from the test environment to the production environment.
B. control the interruption of business operations from lack of attention to unresolved problems.
C. ensure the uninterrupted operation of the business in the event of a disaster.
D. verify that system changes are properly documented.

Answer: A

Explanation:

Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

QUESTION NO: 610

In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

A. application programmer copy the source program and compiled object module to the production libraries.
B. application programmer copy the source program to the production libraries and then have the production control group compile the program.
C. production control group compile the object module to the production libraries using the source program in the test environment.
D. production control group copy the source program to the production libraries and then compile the program.

Answer: D
Explanation:
The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

QUESTION NO: 611

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. Inthis situation, which of the following would be considered an adequate set of compensating controls?

A. Allow changes to be made only with the DBA user account.
B. Make changes to the database after granting access to a normal user account.
C. Use the DBA user account to make changes, log the changes and review the change log the following day.
D. Use the normal user account to make changes, log the changes and review the change log the following day.

Answer: C
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 ofthe DBA user account without logging would permit uncontrolled changes to be made to databases once access to the account was obtained. The use of a normal user account with no restrictions would allow uncontrolled changes to any of the databases. Logging would only provide information on changes made, but would not limit changes to only those that were authorized. Hence, logging coupled with review form an appropriate set of compensating controls.

QUESTION NO: 612

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

A. Review software migration records and verify approvals.
B. identify changes that have occurred and verify approvals.
C. Review change control documentation and verify approvals.
D. Ensure that only appropriate staff can migrate changes into production.

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

QUESTION NO: 613

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?

A. Analyze the need for the structural change.
B. Recommend restoration to the originally designed structure.
C. Recommend the implementation of a change control process.
D. Determine if the modifications were properly approved.

Answer: D
Explanation:
An IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the IS auditor find that the structural modification had not been approved.

QUESTION NO: 614

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?

A. Comparing source code
B. Reviewing system log files
C. Comparing object code
D. Reviewing executable and source code integrity

Answer: B

Explanation:

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

QUESTION NO: 615

The purpose of code signing is to provide assurance that:

A. the software has not been subsequently modified.
B. the application can safely interface with another signed application.
C. the signer of the application is trusted.
D. the private key of the signer has not been compromised.

Answer: A

Explanation:

Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

QUESTION NO: 616

An IS auditor should recommend the use of library control software to provide reasonable assurance that:

A. program changes have been authorized.
B. only thoroughly tested programs are released.
C. modified programs are automatically moved to production.
D. source and executable code integrity is maintained.

Answer: A

Explanation:

Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

QUESTION NO: 617

An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

A. apply the patch according to the patch's release notes.
B. ensure that a good change management process is in place.
C. thoroughly test the patch before sending it to production.
D. approve the patch after doing a risk assessment.

Answer: B

Explanation:

An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly. The other choices are part of a good change management process but arenot an IS auditor's responsibility.

QUESTION NO: 618

When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

A. allow changes, which will be completed using after-the-fact follow-up.
B. allow undocumented changes directly to the production library.
C. do not allow any emergency changes.
D. allow programmers permanent access to production programs.

Answer: A

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 becompleted using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

QUESTION NO: 619

To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

A. examine the change control system records and trace them forward to object code files.
B. review access control permissions operating within the production program libraries.
C. examine object code to find instances of changes and trace them back to change control records.
D. review change approved designations established within the change control system.

Answer: C
Explanation:
The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes. The other choices are valid procedures to apply in a change control audit but they do not directly address the risk of unauthorized code changes.

QUESTION NO: 620

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?

A. Rewrite the patches and apply them
B. Code review and application of available patches
C. Develop in-house patches
D. identify and test suitable patches before applying them

Answer: D
Explanation:
Suitable patches from the existing developers should be selected and tested before applying them.
Rewriting the patches and applying them is not a correct answer because it would require skilled resources and time to rewrite the patches. Code review could be possible but tests need to be performed before applying the patches. Since the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.

QUESTION NO: 621

An IS auditor discovers that developers have operator access to the command line of a

production environment operating system. Which of the following controls wou Id BEST mitigate the risk of undetected and unauthorized program changes to the production environment?

A. Commands typed on the command line are logged
B. Hash keys are calculated periodically for programs and matched against hash keys calculated

for the most recent authorized versions of the programs
C. Access to the operating system command line is granted through an access restriction tool with preapproved rights
D. Software development tools and compilers have been removed from the production environment

Answer: B
Explanation:
The matching of hash keys over time would allow detection of changes to files. Choice A is incorrect because having a log is not a control, reviewing the log is a control. Choice C is incorrect because the access was already granted-it does notmatter how. Choice D is wrong because files can be copied to and from the production environment.

QUESTION NO: 622

Which of the following processes should an IS auditor recommend to assist in the

recording of baselines for software releases?

A. Change management
B. Backup and recovery
C. incident management
D. Configuration management

Answer: D
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 NO: 623

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 byIT of:

A. the training needs for users after applying the patch.
B. any beneficial impact of the patch on the operational systems.
C. delaying deployment until testing the impact of the patch.
D. the necessity of advising end users of new patches.

Answer: C

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 NO: 624

In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?

A. Approve and document the change the next business day
B. Limit developer access to production to a specific timeframe
C. Obtain secondary approval before releasing to production
D. Disable the compiler option in the production machine

Answer: A

Explanation:

It may be appropriate to allow programmers to make emergency changes as long as they are documented and approved after the fact. Restricting release time frame may help somewhat; however, it would not apply to emergency changes and cannot prevent unauthorized release of the programs. Choices C and D are not relevant in an emergency situation.

QUESTION NO: 625

Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?

A. Achieve standards alignment through an increase of resources devoted to the project
B. Align the data definition standards after completion of the project
C. Delay the project until compliance with standards can be achieved
D. Enforce standard compliance by adopting punitive measures against violators

Answer: A

Explanation:

Provided that data architecture, technical, and operational requirements are sufficiently documented, the alignment to standards could be treated as a specific work package assigned to new project resources. The usage of nonstandard data definitionswould lower the efficiency of the new development, and increase the risk of errors in critical business decisions. To change data definition standards after project conclusion (choice B) is risky and is not a viable solution. On the other hand, punishing the violators (choice D) or delaying the project (choice C) would be an inappropriate suggestion because of the likely damage to the entire project profitability.

QUESTION NO: 626

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?

A. Differential reporting
B. False-positive reporting
C. False-negative reporting
D. Less-detail reporting

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

QUESTION NO: 627

The FIRST step in managing the risk of a cyber attack is to:

A. assess the vulnerability impact.
B. evaluate the likelihood of threats.
C. identify critical information assets.
D. estimate potential damage.

Answer: C
Explanation:
The first step in managing risk is the identification and classification of critical information resources (assets). Once the assets have been identified, the process moves onto the identification of threats, vulnerabilities and calculation of potential damages.

QUESTION NO: 628

Which of the following is the MOST effective method for dealing with the spreading of a

network worm that exploits vulnerability in a protocol?

A. Install the vendor's security fix for the vulnerability.
B. Block the protocol traffic in the perimeter firewall.

C. Block the protocol traffic between internal network segments.
D. Stop the service until an appropriate security fix is installed.

Answer: D
Explanation:
Stopping the service and installing the security fix is the safest way to prevent the worm from spreading, if the service is not stopped, installing the fix is not the most effective method because the worm continues spreading until the fix becomes effective. Blocking the protocol on the perimeter does not stop the worm from spreading to the internal network(s). Blocking the protocol helps to slow down the spreading but also prohibits any software that utilizes it from working between segments.

QUESTION NO: 629

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

A. improve internal control procedures.
B. harden the network to industry best practices.
C. highlight the importance of incident response management to management.
D. improve employee awareness of the incident response process.

Answer: A
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 enablesthe 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 improveemployee awareness.

QUESTION NO: 630

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

A. use this information to launch attacks.
B. forward the security alert.
C. implement individual solutions.
D. fail to understand the threat.

Answer: A

Explanation:

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

QUESTION NO: 631

The MAIN criterion for determining the severity level of a service disruption incident is:

A. cost of recovery.
B. negative public opinion.
C. geographic location.
D. downtime.

Answer: D

Explanation:

The longer the period of time a client cannot be serviced, the greater the severity of the incident. The cost of recovery could be minimal yet the service downtime could have a major impact. Negative public opinion is a symptom of an incident. Geographic location does not determine the severity of the incident.

QUESTION NO: 632

Which of the following would be an indicator of the effectiveness of a computer security incident response team?

A. Financial impact per security incident
B. Number of security vulnerabilities that were patched
C. Percentage of business applications that are being protected
D. Number of successful penetration tests

Answer: A

Explanation:

The most important indicator is the financial impact per security incident. Choices B, C and D could be measures of effectiveness of security, but would not be a measure of the effectiveness of a response team.

QUESTION NO: 633

An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

A. the setup is geographically dispersed.
B. the network servers are clustered in a site.
C. a hot site is ready for activation.
D. diverse routing is implemented for the network.

Answer: B
Explanation:
A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backup if a site has been destroyed. A hot site would also be a good alternative for a single point-of-failure site.

QUESTION NO: 634

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

A. Firewalls
B. Routers
C. Layer 2 switches
D. VLANs

Answer: A
Explanation:
Firewall systems are the primary tool that enable an organization to prevent unauthorized access between networks. An organization may choose to deploy one or more systems that function as firewalls. Routers can filter packets based on parameters, such as source address, but are not primarily a security tool. Based on Media Access Control (MAC) addresses, layer 2 switches separate traffic in a port as different segments and without determining if it is authorized or unauthorized traffic. A virtual LAN (VLAN) is a functionality of some switches that allows them to switch the traffic between different ports as if they are in the same LAN. Nevertheless, they do not deal with authorized vs. unauthorized traffic.

QUESTION NO: 635

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

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

Answer: D

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 NO: 636

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:

A. compromises the Wireless Application Protocol (WAP) gateway.
B. installs a sniffing program in front of the server.
C. steals a customer's PDA.
D. listens to the wireless transmission.

Answer: A

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 NO: 637

Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

A. Filters
B. Switches
C. Routers
D. Firewalls

Answer: B

Explanation:

Switches are at the lowest level of network security and transmit a packet to the device to which it is addressed. This reduces the ability of one device to capture the packets that are meant for another device. Filters allow for some basic isolationof network traffic based on the destination addresses. Routers allow packets to be given or denied access based on the addresses of the sender and receiver and the type of packet. Firewalls are a collection of computer and network equipment used toallow communications to flow out of the organization and restrict communications flowing into the organization.

QUESTION NO: 638

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

A. Diskless workstations
B. Data encryption techniques
C. Network monitoring devices
D. Authentication systems

Answer: C

Explanation:

Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations preventaccess 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 environmentwide, logical facilities that can differentiate among users, before providing access to systems.

QUESTION NO: 639

When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

A. they are set to meet security and performance requirements.
B. changes are recorded in an audit trail and periodically reviewed.
C. changes are authorized and supported by appropriate documents.
D. access to parameters in the system is restricted.

Answer: A

Explanation:

The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing them is a detective control; however, if parameters are not set according to business rules, monitoring of changes may not be an effective control. Reviewing changes to ensure they are supported by appropriate documents is also a detective control, if parameters are set incorrectly, the related documentation and the fact that these are authorized does not reduce the impact. Restriction of access to parameters ensures that only authorized staff can access the parameters; however, if the parameters are set incorrectly, restricting access will still have an adverse impact.

QUESTION NO: 640

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

A. Restricting operator access and maintaining audit trails
B. Monitoring and reviewing system engineering activity
C. Providing network redundancy
D. Establishing physical barriers to the data transmitted over the network

Answer: C
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 NO: 641

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?

A. Electromagnetic interference (EMI)
B. Cross-talk
C. Dispersion
D. Attenuation

Answer: D
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 NO: 642

Which of the following line media would provide the BEST security for a telecommunication network?

A. Broadband network digital transmission
B. Baseband network
C. Dial-up
D. Dedicated lines

Answer: D
Explanation:
Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

QUESTION NO: 643

Which of the following types of firewalls would BEST protect a network from an internet attack?

A. Screened subnet firewall
B. Application filtering gateway
C. Packet filtering router
D. Circuit-level gateway

Answer: A
Explanation:
A screened subnet firewall would provide the best protection. The screening router can be a commercial router or a node with routing capabilities and the ability to allow or avoid traffic between nets or nodes based on addresses, ports, protocols, interfaces, etc. Application-level gateways are mediators between two entities that want to communicate, also known as proxy gateways. The application level (proxy) works at the application level, not just at a package level. The screening controls atthe package level, addresses and ports, but does not see the contents of the package. A packet filtering router examines the header of every packet or data traveling between the internet and the corporate network.

QUESTION NO: 644

Neural networks are effective in detecting fraud because they can:

A. discover new trends since they are inherently linear.
B. solve problems where large and general sets of training data are not obtainable.
C. attack problems that require consideration of a large number of input variables.
D. make assumptions about the shape of any curve relating variables to the output.

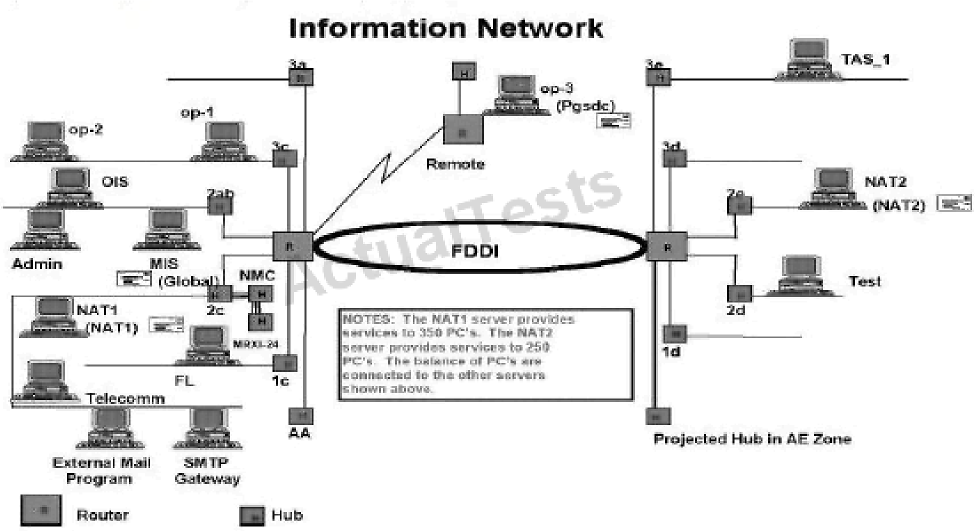
Answer: C

Explanation:

Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

QUESTION NO: 645

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



NOTES: The NAT1 server provides services to 350 PC's. The NAT2 server provides services to 250 PC's. The balance of PC's are connected to the other servers shown above.

A. No firewalls are needed
B. Op-3 location only
C. MIS (Global) and NAT2
D. SMTP Gateway and op-3

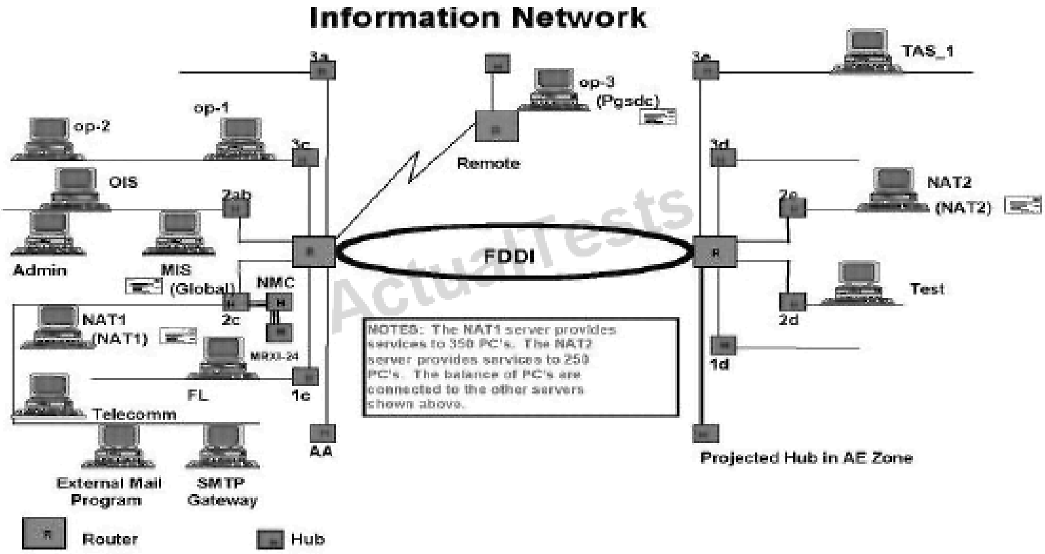
Answer: D

Explanation:

The objective of a firewall is to protect a trusted network from an untrusted network; therefore, locations needing firewall implementations would be at the existence of the external connections. All other answers are incomplete or represent internal connections.

QUESTION NO: 646

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?



NOTES: The NAT1 server provides services to 350 PC's. The NAT2 server provides services to 250 PC's. The balance of PC's are connected to the other servers shown above.

A. Intelligent hub
B. Physical security over the hubs
C. Physical security and an intelligent hub
D. No controls are necessary since this is not a weakness

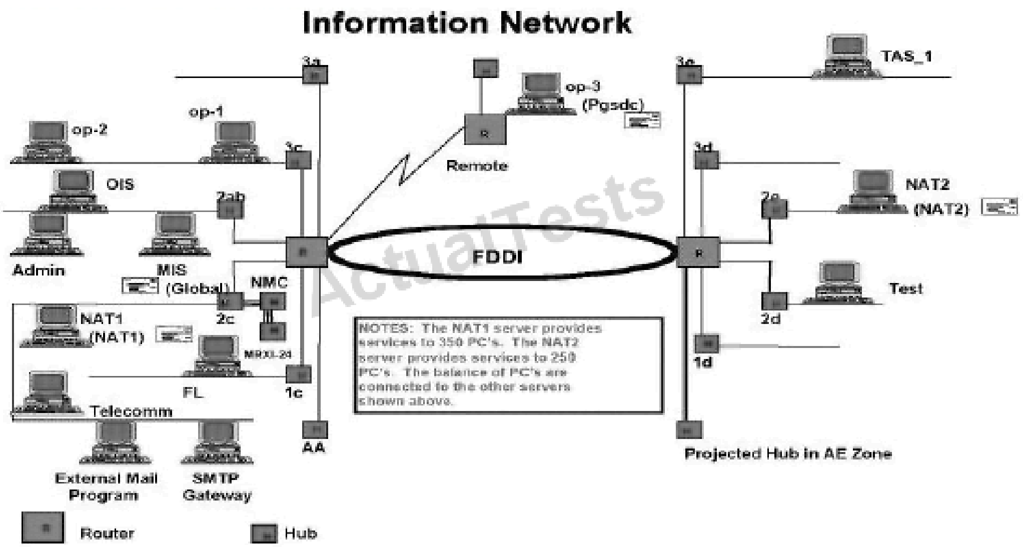
Answer: C

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 NO: 647

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



A. Virus attack
B. Performance degradation
C. Poor management controls
D. Vulnerability to external hackers

Answer: B
Explanation:
Hubs are internal devices that usually have no direct external connectivity, and thus are not prone to hackers. There are no known viruses that are specific to hub attacks. While this situation may be an indicator of poor management controls, choiceB is more likely when the practice of stacking hubs and creating more terminal connections is used.

QUESTION NO: 648

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

Answer: D
Explanation:
The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall

platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

QUESTION NO: 649

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

A. address of the domain server.
B. resolution service for the name/address.
C. IP addresses for the internet.
D. domain name system.

Answer: B
Explanation:
DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

QUESTION NO: 650

In what way is a common gateway interface (CGI) MOST often used on a webserver?

A. Consistent way for transferring data to the application program and back to the user
B. Computer graphics imaging method for movies and TV
C. Graphic user interface for web design
D. interface to access the private gateway domain

Answer: A
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 orentering 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 NO: 651

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

A. translating and unbundling transactions.
B. routing verification procedures.
C. passing data to the appropriate application system.
D. creating a point of receipt audit log.

Answer: B
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 in sending and receiving EDI transactions if they cannot be processed by an internal system. Unpacking transactions and recording audit logs are important elements that help follow business rules and establish controls, but are not part of the communication's interface stage.

QUESTION NO: 652

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

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

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

QUESTION NO: 653
The most likely error to occur when implementing a firewall is:

A. incorrectly configuring the access lists.
B. compromising the passwords due to social engineering.
C. connecting a modem to the computers in the network.
D. inadequately protecting the network and server from virus attacks.

Answer: A

Explanation:

An updated and flawless access list is a significant challenge and, therefore, has the greatest chance for errors at the time of the initial installation. Passwords do not apply to firewalls, a modem bypasses a firewall and a virus attack is not an element in implementing a firewall.

QUESTION NO: 654

When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

A. node list.
B. acceptance test report.
C. network diagram.
D. user's list.

Answer: C

Explanation:

To properly review a LAN implementation, an IS auditor should first verify the network diagram and confirm the approval. Verification of nodes from the node list and the network diagram would be next, followed by a review of the acceptance test report and then the user's list.

QUESTION NO: 655

Which of the following would be the MOST secure firewall system?

A. Screened-host firewall
B. Screened-subnet firewall
C. Dual-homed firewall
D. Stateful-inspection firewall

Answer: B

Explanation:

A screened-subnet firewall, also used as a demilitarized zone (DMZ), utilizes two packet filtering routers and a bastion host. This provides the most secure firewall system, since it supports both network- and application-level security while defining a separate DMZ network. A screened-host firewall utilizes a packet filtering router and a bastion host. This approach implements basic network layer security (packet filtering) and application server security (proxy services). A dual-homed firewall system is a more restrictive form of a screened-host firewall system, configuring one interface for information servers and another for private network host computers. A stateful-inspection firewall working at the transport layer keeps track of thedestination IP address of each packet that leaves the organization's internal network and allows a reply from the recorded IP addresses.

QUESTION NO: 656

Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

A. Circuit gateway
B. Application gateway
C. Packet filter
D. Screening router

Answer: B
Explanation:
An application gateway firewall is effective in preventing applications, such as FTPs, from entering the organization network. A circuit gateway firewall is able to prevent paths or circuits, not applications, from entering the organization's network. A packet filter firewall or screening router will allow or prevent access based on IP packets/address.

QUESTION NO: 657

Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

A. A program that deposits a virus on a client machine
B. Applets recording keystrokes and, therefore, passwords
C. Downloaded code that reads files on a client's hard drive
D. Applets opening connections from the client machine

Answer: D
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 toas 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 NO: 658

Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

A. Simple Network Management Protocol
B. File Transfer Protocol
C. Simple Mail Transfer Protocol
D. Telnet

Answer: A
Explanation:
The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

QUESTION NO: 659

Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

A. a firewall exists.
B. a secure web connection is used.
C. the source of the executable file is certain.
D. the host web site is part of the organization.

Answer: C
Explanation:
Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere. It is virtually impossible at thistime to filter at this level. A secure web connection or firewall is considered an external defense. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither

asecure web connection nor a firewall can identify an executable file as friendly. Hosting the web site as part of the organization is impractical. Enabling the acceptance of Java applets and/or Active X controls is an all-or-nothing proposition. Theclient will accept the program if the parameters are established to do so.

QUESTION NO: 660

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?

A. Appliances
B. Operating system-based
C. Host-based
D. Demilitarized

Answer: A
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 NO: 661

Which of the following types of transmission media provide the BEST security against unauthorized access?

A. Copper wire
B. Twisted pair
C. Fiberoptic cables
D. Coaxial cables

Answer: C
Explanation:
Fiberoptic cables have proven to be more secure than the other mediA. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

QUESTION NO: 662
Which of the following is the BEST audit procedure to determine if a firewall is configured in

compliance with an organization's security policy?

A. Review the parameter settings.
B. Interview the firewall administrator.
C. Review the actual procedures.
D. Review the device's log file for recent attacks.

Answer: A
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 NO: 663

To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

A. business software.
B. infrastructure platform tools.
C. application services.
D. system development tools.

Answer: C
Explanation:
Projects should identify the complexities of the IT Infrastructure that can be simplified or isolated by the development of application services. Application services isolate system developers from the complexities of the IT infrastructure and offercommon functionalities that are shared by many applications. Application services take the form of interfaces, middleware, etc. Business software focuses on business processes, whereas application services bridge the gap between applications and theIT Infrastructure components. Infrastructure platform tools are related to core hardware and software components required for development of the IT infrastructure. Systems development tools represent development components of the IT infrastructure development.

QUESTION NO: 664

During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

A. Storage area network (SAN)
B. Network Attached Storage (NAS)
C. Network file system (NFS v2)
D. Common Internet File System (CIFS)

Answer: A

Explanation:

In contrast to the other options, in a SAN comprised of computers, FC switches or routers and storage devices, there is no computer system hosting and exporting its mounted file system for remote access, aside from special file systems. Access to information stored on the storage devices in a SAN is comparable to direct attached storage, which means that each block of data on a disk can be addressed directly, since the volumes of the storage device are handled as though they are local, thus providing optimal performance. The other options describe technologies in which a computer (or appliance) shares its information with other systems. To access the information, the complete file has to be read.

QUESTION NO: 665

Reverse proxy technology for web servers should be deployed if:

A. http servers' addresses must be hidden.
B. accelerated access to all published pages is required.
C. caching is needed for fault tolerance.
D. bandwidth to the user is limited.

Answer: A

Explanation:

Reverse proxies are primarily designed to hide physical and logical internal structures from outside access. Complete URLs or URIs can be partially or completely redirected without disclosing which internal or DMZ server is providing the requested datA. This technology might be used if a trade-off between security, performance and costs has to be achieved. Proxy servers cache some data but normally cannot cache all pages to be published because this depends on the kind of information the web servers provide. The ability to accelerate access depends on the speed of the back-end servers, i.e., those that are cached. Thus, without making further assumptions, a gain in speed cannot be assured, but visualization and hiding of internal structures can. If speed is an issue, a scale-out approach (avoiding adding additional delays by passing firewalls, involving more servers, etc.) would be a better solution. Due to the limited caching option, reverse proxies are not suitable for enhancing fault tolerance. User requests that are handled by reverse proxy servers are using exactly the same bandwidth as direct requests to the hosts providing the data.

QUESTION NO: 666

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

A. verify that the firewall is not dropping any forwarded packets.
B. review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.

C. verify that the filters applied to services such as HTTP are effective.
D. test whether routing information is forwarded by the firewall.

Answer: C
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 NO: 667

An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

A. Simple Object Access Protocol (SOAP)
B. Address Resolution Protocol (ARP)
C. Routing Information Protocol (RIP)
D. Transmission Control Protocol (TCP)

Answer: B
Explanation:
Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform-independent XML-based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connectionand exchange streams of data.

QUESTION NO: 668

An IS auditor examining the configuration of an operating system to verify the controls should review the:

A. transaction logs.
B. authorization tables.
C. parameter settings.
D. routing tables.

Answer: C
Explanation:

Parameters allow a standard piece of software to be customized for diverse environments and are important in determining how a system runs. The parameter settings should be appropriate to an organization's workload and control environment, improper implementation and/or monitoring of operating systems can result in undetected errors and corruption of the data being processed, as well as lead to unauthorized access and inaccurate logging of system usage. Transaction logs are used to analyze transactions in master and/or transaction files. Authorization tables are used to verify implementation of logical access controls and will not be of much help when reviewing control features of an operating system. Routing tables do not contain information about the operating system and, therefore, provide no information to aid in the evaluation of controls.

QUESTION NO: 669

When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

A. an integrated services digital network (ISDN) data link.
B. traffic engineering.
C. wired equivalent privacy (WEP) encryption of data.
D. analog phone terminals.

Answer: B
Explanation:
To ensure that quality of service requirements are achieved, the Voice-over IP (VoIP) service over the wide area network (WAN) should be protected from packet losses, latency or jitter. To reach this objective, the network performance can be managedusing statistical techniques such as traffic engineering. The standard bandwidth of an integrated services digital network (ISDN) data link would not provide the quality of services required for corporate VoIP services. WEP is an encryption scheme related to wireless networking. The VoIP phones are usually connected to a corporate local area network (LAN) and are not analog.

QUESTION NO: 670

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

A. Session keys are dynamic
B. Private symmetric keys are used
C. Keys are static and shared
D. Source addresses are not encrypted or authenticated

Answer: A
Explanation:
WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy

(WEP), which operates with static keys (same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

QUESTION NO: 671

During the audit of a database server, which of the following would be considered the GREATEST exposure?

A. The password does not expire on the administrator account
B. Default global security settings for the database remain unchanged
C. Old data have not been purged
D. Database activity is not fully logged

Answer: B
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 isnot an immediate security concern. Choice A is an exposure but not as serious as B.

QUESTION NO: 672

Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

A. A user from within could send a file to an unauthorized person.
B. FTP services could allow a user to download files from unauthorized sources.
C. A hacker may be able to use the FTP service to bypass the firewall.
D. FTP could significantly reduce the performance of a DMZ server.

Answer: C
Explanation:
Since file transfer protocol (FTP) is considered an insecure protocol, it should not be installed on a server in a demilitarized zone (DMZ). FTP could allow an unauthorized user to gain access to the 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 NO: 673

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

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

Answer: D
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-mailmay not be accurate, this is not a significant issue.

QUESTION NO: 674

When reviewing the configuration of network devices, an IS auditor should FIRST identify:

A. the best practices for the type of network devices deployed.
B. whether components of the network are missing.
C. the importance of the network device in the topology.
D. whether subcomponents of the network are being used appropriately.

Answer: C
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.

Topic 6, PROTECTION OF INFORMATION ASSETS (251 PRACTICE QUESTIONS)

QUESTION NO: 675

Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

A. System analysis
B. Authorization of access to data

C. Application programming
D. Data administration

Answer: B
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 NO: 676

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

A. security administrator.
B. systems administrator.
C. data and systems owners.
D. systems operations group.

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

QUESTION NO: 677

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:

A. make unauthorized changes to the database directly, without an audit trail.
B. make use of a system query language (SQL) to access information.
C. remotely access the database.
D. update data without authentication.

Answer: A
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 NO: 678

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

A. activity lists.
B. access control lists.
C. logon ID lists.
D. password lists.

Answer: B

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.

QUESTION NO: 679

Which of the following is the MOST effective control when granting temporary access to vendors?

A. Vendor access corresponds to the service level agreement (SLA).
B. User accounts are created with expiration dates and are based on services provided.
C. Administrator access is provided for a limited period.
D. User IDs are deleted when the work is completed.

Answer: B

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 Dsafter the work is completed is necessary, but if not automated, the deletion could be overlooked.

QUESTION NO: 680

During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

A. an unauthorized user may use the ID to gain access.
B. user access management is time consuming.
C. passwords are easily guessed.
D. user accountability may not be established.

Answer: D
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 NO: 681

Which of the following satisfies a two-factor user authentication?

A. Iris scanning plus fingerprint scanning
B. Terminal ID plus global positioning system (GPS)
C. A smart card requiring the user's PIN
D. User ID along with password

Answer: C
Explanation:
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). Proving who the user is usually requires a biometrics method, such as fingerprint, iris scan or voice verification, to prove biology. This is not a two-factor user authentication, because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. The use of an ID and password (what the user knows) is a single-factor user authentication.

QUESTION NO: 682

What is the MOST effective method of preventing unauthorized use of data files?

A. Automated file entry
B. Tape librarian
C. Access control software
D. Locked library

Answer: C

Explanation:

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

QUESTION NO: 683

Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?

A. Security awareness
B. Reading the security policy
C. Security committee
D. Logical access controls

Answer: D

Explanation:

To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserve the confidentiality of sensitive data and ensure the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent the unauthorized access of information. A security committee (choice C) is key to the protection of information assets, butwould address security issues within a broader perspective.

QUESTION NO: 684

Which of the following is a benefit of using a callback device?

A. Provides an audit trail
B. Can be used in a switchboard environment
C. Permits unlimited user mobility
D. Allows call forwarding

Answer: A

Explanation:

A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting the follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

QUESTION NO: 685

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

A. Passwords are not shared.
B. Password files are not encrypted.
C. Redundant logon IDs are deleted.
D. The allocation of logon IDs is controlled.

Answer: B
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 NO: 686

Passwords should be:

A. assigned by the security administrator for first time logon.
B. changed every 30 days at the discretion of the user.
C. reused often to ensure the user does not forget the password.
D. displayed on the screen so that the user can ensure that it has been entered properly.

Answer: A
Explanation:
Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

QUESTION NO: 687

When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?

A. Read access to data
B. Delete access to transaction data files
C. Logged read/execute access to programs

D. Update access to job control language/script files

Answer: B

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 controljob execution.

QUESTION NO: 688

To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:

A. online terminals are placed in restricted areas.
B. online terminals are equipped with key locks.
C. ID cards are required to gain access to online terminals.
D. online access is terminated after a specified number of unsuccessful attempts.

Answer: D

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 NO: 689

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:

A. exposure is greater, since information is available to unauthorized users.
B. operating efficiency is enhanced, since anyone can print any report at any time.
C. operating procedures are more effective, since information is easily available.
D. user friendliness and flexibility is facilitated, since there is a smooth flow of information among users.

Answer: A

Explanation:

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

QUESTION NO: 690

Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:

A. change the company's security policy.
B. educate users about the risk of weak passwords.
C. build in validations to prevent this during user creation and password change.
D. require a periodic review of matching user ID and passwords for detection and correction.

Answer: C
Explanation:
The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

QUESTION NO: 691

The PRIMARY objective of a logical access control review is to:

A. review access controls provided through software.
B. ensure access is granted per the organization's authorities.
C. walk through and assess the access provided in the IT environment.
D. provide assurance that computer hardware is adequately protected against abuse.

Answer: B
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 NO: 692

Naming conventions for system resources are important for access control because they:

A. ensure that resource names are not ambiguous.

B. reduce the number of rules required to adequately protect resources.
C. ensure that user access to resources is clearly and uniquely identified.
D. ensure that internationally recognized names are used to protect resources.

Answer: B

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 handledby access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

QUESTION NO: 693

Which of the following exposures could be caused by a line grabbing technique?

A. Unauthorized data access
B. Excessive CPU cycle usage
C. Lockout of terminal polling
D. Multiplexor control dysfunction

Answer: A

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 NO: 694

Electromagnetic emissions from a terminal represent an exposure because they:

A. affect noise pollution.
B. disrupt processor functions.
C. produce dangerous levels of electric current.
D. can be detected and displayed.

Answer: D

Explanation:

Emissions can be detected by sophisticated equipment and displayed, thus giving unauthorized persons access to datA. They should not cause disruption of CPUs or effect noise pollution.

QUESTION NO: 695

Security administration procedures require read-only access to:

A. access control tables.
B. security log files.
C. logging options.
D. user profiles.

Answer: B
Explanation:
Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update the way the transactions and user activities aremonitored, captured, stored, processed and reported.

QUESTION NO: 696

With the help of a security officer, granting access to data is the responsibility of:

A. data owners.
B. programmers.
C. system analysts.
D. librarians.

Answer: A
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 NO: 697

The FIRST step in data classification is to:

A. establish ownership.

B. perform a criticality analysis.
C. define access rules.
D. create a data dictionary.

Answer: A
Explanation:
Data classification is necessary to define access rules based on a need-to-do and need-to-know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for protection of data, which takes input from data classification. Access definition is complete after data classification and input for a data dictionary is prepared from the data classification process.

QUESTION NO: 698

Which of the following provides the framework for designing and developing logical access controls?

A. Information systems security policy
B. Access control lists
C. Password management
D. System configuration files

Answer: A
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 aretools for implementing the access controls.

QUESTION NO: 699

A hacker could obtain passwords without the use of computer tools or programs through the technique of:

A. social engineering.
B. sniffers.
C. back doors.
D. Trojan horses.

Answer: A
Explanation:
Social engineering is based on the divulgence of private information through dialogues, interviews,

inquiries, etc., in which a user may be indiscreet regarding their or someone else's personal datA. A sniffer is a computer tool to monitor the traffic in networks. Back doors are computer programs left by hackers to exploit vulnerabilities. Trojan horses are computer programs that pretend to supplant a real program; thus, the functionality of the program is not authorized and is usually maliciousin nature.

QUESTION NO: 700

The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trail.
B. the security administrator has read-only rights to the audit file.
C. date and time stamps are recorded when an action occurs.
D. users can amend audit trail records when correcting system errors.

Answer: D
Explanation:
An audit trail is not effective if the details in it can be amended.

QUESTION NO: 701

Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?

A. Three users with the ability to capture and verify their own messages
B. Five users with the ability to capture and send their own messages
C. Five users with the ability to verify other users and to send their own messages
D. Three users with the ability to capture and verify the messages of other users and to send their own messages

Answer: A
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 NO: 702

An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:

A. critical.
B. vital.
C. sensitive.

D. noncritical.

Answer: C

Explanation:

Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot bereplaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time; this is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for anextended period of time at little or no cost to the company, and require little time or cost to restore.

QUESTION NO: 703

The implementation of access controls FIRST requires:

A. a classification of IS resources.
B. the labeling of IS resources.
C. the creation of an access control list.
D. an inventory of IS resources.

Answer: D

Explanation:

QUESTION NO: 704

Which of the following is an example of the defense in-depth security principle?

A. Using two firewalls of different vendors to consecutively check the incoming network traffic
B. Using a firewall as well as logical access controls on the hosts to control incoming network traffic
C. Having no physical signs on the outside of a computer center building
D. Using two firewalls in parallel to check different types of incoming traffic

Answer: B

Explanation:

Defense in-depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products the probability of both products having the same vulnerabilities is diminished. Havingno physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

QUESTION NO: 705

Which of the following would be the BEST access control procedure?

A. The data owner formally authorizes access and an administrator implements the user authorization tables.
B. Authorized staff implements the user authorization tables and the data owner sanctions them.
C. The data owner and an IS manager jointly create and update the user authorization tables.
D. The data owner creates and updates the user authorization tables.

Answer: A
Explanation:
The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedurefor authorizing access.

QUESTION NO: 706

Which of the following would MOST effectively reduce social engineering incidents?

A. Security awareness training
B. increased physical security measures
C. E-mail monitoring policy
D. intrusion detection systems

Answer: A
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 NO: 707

An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

Answer: C
Explanation:
If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' thenit would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

QUESTION NO: 708

To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be changed.
B. passwords are periodically changed.
C. an automated password management tool be used.
D. security awareness training is delivered.

Answer: C
Explanation:
The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

QUESTION NO: 709

An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

A. more than one individual can claim to be a specific user.
B. there is no way to limit the functions assigned to users.
C. user accounts can be shared.
D. users have a need-to-know privilege.

Answer: B

Explanation:

Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather thanwith authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

QUESTION NO: 710

An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

A. Digitalized signatures
B. Hashing
C. Parsing
D. Steganography

Answer: D

Explanation:

Steganography is a technique for concealing the existence of messages or information. An increasingly important steganographical 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 NO: 711

The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Answer: A

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have theirbadge read at every controlled door no unauthorized person could enter the sensitive areA. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking,but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

QUESTION NO: 712

Which of the following presents an inherent risk with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

Answer: C
Explanation:
Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the datA. There are only compensatingcontrols for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-re plicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdownof an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which iseffective if there are proper access controls.

QUESTION NO: 713

Which of the following is a general operating system access control function?

A. Creating database profiles
B. Verifying user authorization at a field level
C. Creating individual accountability
D. Logging database access activities for monitoring access violation

Answer: C
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 NO: 714

Which of the following BEST restricts users to those functions needed to perform their duties?

A. Application level access control
B. Data encryption
C. Disabling floppy disk drives
D. Network monitoring device

Answer: A
Explanation:
The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

QUESTION NO: 715

For a discretionary access control to be effective, it must:

A. operate within the context of mandatory access controls.
B. operate independently of mandatory access controls.
C. enable users to override mandatory access controls when necessary.
D. be specifically permitted by the security policy.

Answer: A
Explanation:
Mandatory access controls are prohibitive; anything that is not expressly permitted is forbidden. Only within this context do discretionary controls operate, prohibiting still more access with the same exclusionary principle. When systems enforce mandatory access control policies, they must distinguish between these and the mandatory access policies that offer more flexibility. Discretionary controls do not override access controls and they do not have to be permitted in the

security policy to be effective.

QUESTION NO: 716

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. Ofthe following, which is the BEST control against this risk?

A. Kerberos
B. Vitality detection
C. Multimodal biometrics
D. Before-image/after-image logging

Answer: A
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 NO: 717

From a control perspective, the PRIMARY objective of classifying information assets is to:

A. establish guidelines for the level of access controls that should be assigned.
B. ensure access controls are assigned to all information assets.
C. assist management and auditors in risk assessment.
D. identify which assets need to be insured against losses.

Answer: A
Explanation:
Information has varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources, management can establish guidelines for the level of access controls that should be assigned. End user management and the security administrator will use these classifications in their risk assessment process to assign a given class to each asset.

QUESTION NO: 718

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:

A. all system access is authorized and appropriate for an individual's role and responsibilities.
B. management has authorized appropriate access for all newly-hired individuals.
C. only the system administrator has authority to grant or modify access to individuals.
D. access authorization forms are used to grant or modify access to individuals.

Answer: A
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 NO: 719

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

A. denial of service.
B. an asynchronous attack.
C. wire tapping.
D. computer shutdown.

Answer: B
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 savesa 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 NO: 720

Inadequate programming and coding practices introduce the risk of:

A. phishing.
B. buffer overflow exploitation.

C. SYN flood.
D. brute force attacks.

Answer: B
Explanation:
Buffer overflow exploitation may occur when programs do not check the length of the data that are input into a program. An attacker can send data that exceed the length of a buffer and override part of the program with malicious code. The countermeasure is proper programming and good coding practices. Phishing, SYN flood and brute force attacks happen independently of programming and coding practices.

QUESTION NO: 721

Which of the following would prevent unauthorized changes to information stored in a server's log?

A. Write-protecting the directory containing the system log
B. Writing a duplicate log to another server
C. Daily printing of the system log
D. Storing the system log in write-once media

Answer: D
Explanation:
Storing the system log in write-once media ensures the log cannot be modified. Write-protecting the system log does not prevent deletion or modification, since the superuser or users that have special permission can override the write protection. Writing a duplicate log to another server or daily printing of the system log cannot prevent unauthorized changes.

QUESTION NO: 722

After reviewing its business processes, a large organization is deploying a new web application based on a VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?

A. Fine-grained access control
B. Role-based access control (RBAC)
C. Access control lists
D. Network/service access control

Answer: B
Explanation:
Authorization in this VoIP case can best be addressed by role-based access control (RBAC) technology. RBAC is easy to manage and can enforce strong and efficient access controls in large-scale web environments including VoIP implementation. Access control lists and fine-grained

access control on VoIP web applications do not scale to enterprisewide systems, because they are primarily based on individual user identities and their specific technical privileges. Network/service addresses VoIP availability but does not address application-level access or authorization.

QUESTION NO: 723

In an online banking application, which of the following would BEST protect against identity theft?

A. Encryption of personal password
B. Restricting the user to a specific terminal
C. Two-factor authentication
D. Periodic review of access logs

Answer: C
Explanation:
Two-factor authentication requires two independent methods for establishing identity and privileges. Factors include something you know, such as a password; something you have, such as a token; and something you are, which is biometric. Requiring twoof these factors makes identity theft more difficult. A password could be guessed or broken. Restricting the user to a specific terminal is not a practical alternative for an online application. Periodic review of access logs is a detective controland does not protect against identity theft.

QUESTION NO: 724

Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?

A. Encrypt the hard disk with the owner's public key.
B. Enable the boot password (hardware-based password).
C. Use a biometric authentication device.
D. Use two-factor authentication to logon to the notebook.

Answer: A
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 Ddeal 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 NO: 725

The responsibility for authorizing access to application data should be with the:

A. data custodian.
B. database administrator (DBA).
C. data owner.
D. security administrator.

Answer: C

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) isresponsible 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 NO: 726

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?

A. Look for compensating controls.
B. Review financial transactions logs.
C. Review the scope of the audit.
D. Ask the administrator to disable these accounts.

Answer: A

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 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 NO: 727

Minimum password length and password complexity verification are examples of:

A. detection controls.
B. control objectives.
C. audit objectives.
D. control procedures.

Answer: D

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 NO: 728

An IS auditor finds that a DBA has read and write access to production datA. The IS auditor should:

A. accept the DBA access as a common practice.
B. assess the controls relevant to the DBA function.
C. recommend the immediate revocation of the DBA access to production data.
D. review user access authorizations approved by the DBA.

Answer: B

Explanation:

It is good practice when finding a potential exposure to look for the best controls. Though granting the database administrator (DBA) access to production data might be a common practice, the IS auditor should evaluate the relevant controls. The DBAshould have access based on a need-to-know and need-to-do basis; therefore, revocation may remove the access required. The DBA, typically, may need to have access to some production datA. Granting user authorizations is the responsibility of the dataowner and not the DBA.

QUESTION NO: 729

When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:

A. carry the flash drive in a portable safe.
B. assure management that you will not lose the flash drive.
C. request that management deliver the flash drive by courier.
D. encrypt the folder containing the data with a strong key.

Answer: D

Explanation:

Encryption, with a strong key, is the most secure method for protecting the information on the flash drive. Carrying the flash drive in a portable safe does not guarantee the safety of the information in the event that the safe is stolen or lost. Nomatter what measures you take, the chance of losing the flash drive still exists. It is possible that a courier might lose the flash drive or that it might be stolen.

QUESTION NO: 730

A business application system accesses a corporate database using a single ID and password embedded in a program. Which of the following would provide efficient access control over the organization's data?

A. Introduce a secondary authentication method such as card swipe
B. Apply role-based permissions within the application system
C. Have users input the ID and password for each database transaction
D. Set an expiration period for the database password embedded in the program

Answer: B

Explanation:

When a single ID and password are embedded in a program, the best compensating control would be a sound access control over the application layer and procedures to ensure access to data is granted based on a user's role. The issue is user permissions, not authentication, therefore adding a stronger authentication does not improve the situation. Having a user input the ID and password for access would provide a better control because a database log would identify the initiator of the activity. However, this may not be efficient because each transaction would require a separate authentication process. It is a good practice to set an expiration date for a password. However, this might not be practical for an ID automatically logged in from the program. Often, this type of password is set not to expire.

QUESTION NO: 731

Which of the following is the BEST practice to ensure that access authorizations are still valid?

A. information owner provides authorization for users to gain access
B. identity management is integrated with human resource processes
C. information owners periodically review the access controls
D. An authorization matrix is used to establish validity of access

Answer: B

Explanation:

Personnel and departmental changes can result in authorization creep and can impact the effectiveness of access controls. Many times when personnel leave an organization, or employees are promoted, transferred or demoted, their system access is not fully removed, which increases the risk of unauthorized access. The best practices for ensuring access authorization is still valid is to integrate identity management with human resources processes. When an employee transfers to a different function,access rights are adjusted at the same time.

QUESTION NO: 732

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 discoveredduring a forensic investigation?

A. Audit logs are not enabled for the system
B. A logon ID for the technical lead still exists
C. Spyware is installed on the system
D. A Trojan is installed on the system

Answer: A
Explanation:
Audit logs are critical to the investigation of the event; however, if not enabled, misuse of the logon ID of the technical lead and the guest account could not be established. The logon ID of the technical lead should have been deleted as soon as the employee left the organization but, without audit logs, misuse of the ID is difficult to prove. Spyware installed on the system is a concern but could have been installed by any user and, again, without the presence of logs, discovering who installed the spyware is difficult. A Trojan installed on the system is a concern, but it can be done by any user as it is accessible to the whole group and, without the presence of logs, investigation would be difficult.

QUESTION NO: 733

An organization is using an enterprise resource management (ERP) application. Which of the following would be an effective access control?

A. User-level permissions
B. Role-based
C. Fine-grained
D. Discretionary

Answer: B
Explanation:
Role-based access controls the system access by defining roles for a group of users. Users are assigned to the various roles and the access is granted based on the user's role. User-level permissions for an ERP system would create a larger administrative overhead. Fine-grained

access control is very difficult to implement and maintain in the context of a large enterprise. Discretionary access control may be configured or modified by the users or data owners, and therefore may create inconsistencies in the access control management.

QUESTION NO: 734

What should be the GREATEST concern to an IS auditor when employees use portable media (MP3 players, flash drives)?

A. The copying of sensitive data on them
B. The copying of songs and videos on them
C. The cost of these devices multiplied by all the employees could be high
D. They facilitate the spread of malicious code through the corporate network

Answer: A
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 aless important risk than information leakage. Choice C is hardly an issue because employees normally buy the portable media with their own funds. Choice D is a possible risk, but not as important as information leakage and can be reduced by other controls.

QUESTION NO: 735

An IS auditor should expect the responsibility for authorizing access rights to production

data and systems to be entrusted to the:

A. process owners.
B. system administrators.
C. security administrator.
D. data owners.

Answer: D
Explanation:
Data owners are primarily responsible for safeguarding the data and authorizing access to production data on a need-to-know basis.

QUESTION NO: 736

An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?

A. Network workstations are not disabled automatically after a period of inactivity.
B. Wiring closets are left unlocked
C. Network operating manuals and documentation are not properly secured.
D. Network components are not equipped with an uninterruptible power supply.

Answer: A
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 NO: 737

Which of the following would MOST effectively enhance the security of a challenge-response based authentication system?

A. Selecting a more robust algorithm to generate challenge strings
B. implementing measures to prevent session hijacking attacks
C. increasing the frequency of associated password changes
D. increasing the length of authentication strings

Answer: B
Explanation:
Challenge response-based authentication is prone to session hijacking or man-in-the-middle attacks. Security management should be aware of this and engage in risk assessment and control design when they employ this technology. Selecting a more robust algorithm will enhance the security; however, this may not be as important in terms of risk when compared to man-in-the-middle attacks. Choices C and D are good security practices; however, they are not as effective a preventive measure. Frequently changing passwords is a good security practice; however, the exposures lurking in communication pathways may pose a greater risk.

QUESTION NO: 738

Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

A. implement column- and row-level permissions
B. Enhance user authentication via strong passwords
C. Organize the data warehouse into subject matter-specific databases
D. Log user access to the data warehouse

Answer: A

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

QUESTION NO: 739

The responsibility for authorizing access to a business application system belongs to the:

A. data owner.
B. security administrator.
C. IT security manager.
D. requestor's immediate supervisor.

Answer: A

Explanation:

When a business application is developed, the best practice is to assign an information or data owner to the application. The Information owner should be responsible for authorizing access to the application itself or to back-end databases for queries. Choices B and C are not correct because the security administrator and manager normally do not have responsibility for authorizing access to business applications. The requestor's immediate supervisor may share the responsibility for approving user access to a business application system; however, the final responsibility should go to the information owner.

QUESTION NO: 740

An organization has created a policy that defines the types of web sites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

A. Stateful inspection firewall
B. Web content filter
C. Web cache server
D. Proxy server

Answer: B
Explanation:
A web content filter accepts or denies web communications according to the configured rules. To help the administrator properly configure the tool, organizations and vendors have made available URL blacklists and classifications for millions of web sites. A stateful inspection firewall is of little help in filtering web traffic since it does not review the content of the web site nor does it take into consideration the sites classification. A web cache server is designed to improve the speed of retrieving the most common or recently visited web pages. A proxy server is incorrect because a proxy server is a server which services the request of its clients by forwarding requests to other servers. Many people incorrectly use proxy server as a synonym of web proxy server even though not all web proxy servers have content filtering capabilities.

QUESTION NO: 741

What would be the MOST effective control for enforcing accountability among database users accessing sensitive information?

A. implement a log management process
B. implement a two-factor authentication
C. Use table views to access sensitive data
D. Separate database and application servers

Answer: A
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 NO: 742

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

A. Signature-based
B. Neural networks-based
C. Statistical-based
D. Host-based

Answer: B
Explanation:
The neural networks-based IDS monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but has the added function of self-learning. Signature-based systems are a type of IDS in which the intrusive patterns identified are stored in the form of signatures. These IDS systems protect against detected intrusion patterns. Statistical-based systems need a comprehensive definition of the known and expected behavior of systems. Host-based systems are not a type of IDS, but a category of IDS, and are configured for a specific environment. They will monitor various internal resources of the operating system to warn of a possible attack.

QUESTION NO: 743

The MOST important difference between hashing and encryption is that hashing:

A. is irreversible.
B. output is the same length as the original message.
C. is concerned with integrity and security.
D. is the same at the sending and receiving end.

Answer: A
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, whileencryption 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 usedto 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 end to encrypt and decrypt.

QUESTION NO: 744

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

A. The encryption is symmetric rather than asymmetric.
B. A long asymmetric encryption key is used.

C. The hash is encrypted rather than the message.
D. A secret key is used.

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

QUESTION NO: 745

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

A. the documentation of the planned testing procedure.
B. scheduling and deciding on the timed length of the test.
C. the involvement of the management of the client organization.
D. the qualifications and experience of staff involved in the test.

Answer: C
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 NO: 746

Which of the following virus prevention techniques can be implemented through hardware?

A. Remote booting
B. Heuristic scanners
C. Behavior blockers
D. Immunizers

Answer: A
Explanation:
Remote booting (e.g., diskless workstations) is a method of preventing viruses, and can be implemented through hardware. Choice C is a detection, not a prevention, although it is hardware-based. Choices B and D are not hard ware-based.

QUESTION NO: 747

Which of the following append themselves to files as a protection against viruses?

A. Behavior blockers
B. Cyclical redundancy checkers (CRCs)
C. Immunizers
D. Active monitors

Answer: C
Explanation:
I mmunizers 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 NO: 748

Which of the following acts as a decoy to detect active internet attacks?

A. Honeypots
B. Firewalls
C. Trapdoors
D. Traffic analysis

Answer: A
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 NO: 749

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

A. revocation and suspension of a subscriber's certificate.
B. generation and distribution of the CA public key.
C. establishing a link between the requesting entity and its public key.
D. issuing and distributing subscriber certificates.,

Answer: C
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 NO: 750

Which of the following results in a denial-of-service attack?

A. Brute force attack
B. Ping of death
C. Leapfrog attack
D. Negative acknowledgement (NAK) attack

Answer: B
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 telneting through one or more hosts to preclude a trace, makes use of user ID and password information obtained illicitly from one host to compromise another host. A negative acknowledgement attack is a penetration technique that capitalizes on a potential weakness in an operating system that does not handle asynchronous interrupts properly, leaving the system in an unprotected state during such interrupts.

QUESTION NO: 751

Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

A. Computation speed
B. Ability to support digital signatures
C. Simpler key distribution
D. Greater strength for a given key length

Answer: A

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 NO: 752

Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability and integrity of data?

A. Secure Sockets Layer (SSL)
B. Intrusion detection system (IDS)
C. Public key infrastructure (PKI)
D. Virtual private network (VPN)

Answer: C

Explanation:

PKI would be the best overall technology because cryptography provides for encryption, digital signatures and non repudiation controls for confidentiality and reliability. SSL can provide confidentiality. IDS is a detective control. A VPN would provide confidentiality and authentication (reliability).

QUESTION NO: 753

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:

A. 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.
B. 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.
C. 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.
D. the entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Answer: A

Explanation:

Applying a cryptographic hashing algorithm against the entire message addresses the message integrity issue. Enciphering the message digest using the sender's private key addresses non repudiation. Encrypting the message with a symmetric key, thereafter allowing the key to be enciphered using the receiver's public key, most efficiently addresses the confidentiality of the message as well as the receiver's non repudiation. The other choices would address only a portion of the requirements.

QUESTION NO: 754

Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

A. Server antivirus software
B. Virus walls
C. Workstation antivirus software
D. Virus signature updating

Answer: B

Explanation:

An important means of controlling the spread of viruses is to detect the virus at the point of entry, before it has an opportunity to cause damage. In an interconnected corporate network, virus scanning software, used as an integral part of firewall technologies, is referred to as a virus wall. Virus walls scan incoming traffic with the intent of detecting and removing viruses before they enter the protected network. The presence of virus walls does not preclude the necessity for installing virus detection software on servers and workstations within the network, but network-level protection is most effective the earlier the virus is detected. Virus signature updating is a must in all circumstances, networked or not.

QUESTION NO: 755

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:

A. on the enterprise's internal network.
B. at the backup site.
C. in employees' homes.
D. at the enterprise's remote offices.

Answer: C

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 NO: 756

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

A. confidentiality.
B. integrity.
C. availability.
D. timeliness.

Answer: B
Explanation:
Digital signatures provide integrity because the digital signature of a signed message (file, mail, document, etc.) changes every time a single bit of the document changes; thus, a signed document cannot be altered. Depending on the mechanism chosen to implement a digital signature, the mechanism might be able to ensure data confidentiality or even timeliness, but this is not assured. Availability is not related to digital signatures.

QUESTION NO: 757

Which of the following is an example of a passive attack initiated through the Internet?

A. Traffic analysis
B. Masquerading
C. Denial of service
D. E-mail spoofing

Answer: A
Explanation:
Internet security threats/vulnerabilities are divided into passive and active attacks. Examples of

passive attacks include network analysis, eavesdropping and traffic analysis. Active attacks include brute force attacks, masquerading, packet replay, message modification, unauthorized access through the Internet or web-based services, denial-of-service attacks, dial-in penetration attacks, e-mail bombing and spamming, and e-mail spoofing.

QUESTION NO: 758

Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called a:

A. feedback error control.
B. block sum check.
C. forward error control.
D. cyclic redundancy check.

Answer: C
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 NO: 759

The security level of a private key system depends on the number of:

A. encryption key bits.
B. messages sent.
C. keys.
D. channels used.

Answer: A
Explanation:
The security level of a private key system depends on the number of encryption key bits. The larger the number of bits, the more difficult it would be to understand or determine the algorithm. The security of the message will depend on the encryption key bits used. More than keys by themselves, the algorithm and its complexity make the content more secured. Channels, which could be open or secure, are the mode for sending the message.

QUESTION NO: 760

During what process should router access control lists be reviewed?

A. Environmental review
B. Network security review
C. Business continuity review
D. Data integrity review

Answer: B
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 NO: 761

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

A. Analyzer
B. Administration console
C. User interface
D. Sensor

Answer: D
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 NO: 762

Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

A. Unauthorized access from outside the organization
B. Unauthorized access from within the organization
C. A delay in Internet connectivity
D. A delay in downloading using File Transfer Protocol (FTP)

Answer: A
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 NO: 763

A digital signature contains a message digest to:

A. show if the message has been altered after transmission.
B. define the encryption algorithm.
C. confirm the identity of the originator.
D. enable message transmission in a digital format.

Answer: A
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 indigital format and has no effect on the identity of the user; it is there to ensure integrity rather than identity.

QUESTION NO: 764

Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

A. Registration authority
B. Certificate authority (CA)
C. Certification relocation list
D. Certification practice statement

Answer: B
Explanation:
The certificate authority maintains a directory of digital certificates for the reference of those receiving them, it manages the certificate life cycle, including certificate directory maintenance and certificate revocation list maintenance and publication. Choice A is not correct because a registration authority is an optional entity that is responsible for the administrative tasks associated with registering the end entity that is the subject of the certificate issued by the CA. Choice C is incorrect since a CRL is an instrument for checking the continued validity of the certificates for which the CA has responsibility. Choice D is incorrect because a certification practice statement is a detailed set of rules governing the certificate authority's operations.

QUESTION NO: 765

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?

A. Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).
B. A digital signature with RSA has been implemented.
C. Digital certificates with RSA are being used.
D. Work is being completed in TCP services.

Answer: A
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 NO: 766

Digital signatures require the:

A. signer to have a public key and the receiver to have a private key.
B. signer to have a private key and the receiver to have a public key.
C. signer and receiver to have a public key.
D. signer and receiver to have a private key.

Answer: B
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 NO: 767

The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

A. data integrity.
B. authentication.
C. non repudiation.
D. replay protection.

Answer: C
Explanation:
All of the above are features of a digital signature. Non repudiation ensures that the claimed

sender cannot later deny generating and sending the message. Data integrity refers to changes in the plaintext message that would result in the recipient failing to compute the same message hash. Since only the claimed sender has the key, authentication ensures that the message has been sent by the claimed sender. Replay protection is a method that a recipient can use to check that the message was not intercepted and replayed.

QUESTION NO: 768

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

A. evaluate configurations.
B. examine security settings.
C. ensure virus-scanning software is in use.
D. use tools and techniques available to a hacker.

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

QUESTION NO: 769

Which of the following should concern an IS auditor when reviewing security in a client-server environment?

A. Protecting data using an encryption technique
B. Preventing unauthorized access using a diskless workstation
C. The ability of users to access and modify the database directly
D. Disabling floppy drives on the users' machines

Answer: C
Explanation:
For the purpose of data security in a client-server environment, an IS auditor should be concerned with the users ability to access and modify a database directly. This could affect the integrity of the data in the database. Data protected by encryption aid in securing the datA. Diskless workstations prevent copying of data into local disks and thus help to maintain the integrity and confidentiality of datA. Disabling floppy drives is a physical access control, which helps to maintain the confidentiality of data by preventing it from being copied onto a disk.

QUESTION NO: 770

Which of the following is a technique that could be used to capture network user passwords?

A. Encryption
B. Sniffing
C. Spoofing
D. Data destruction

Answer: B
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 NO: 771

Which of the following controls would BEST detect intrusion?

A. User IDs and user privileges are granted through authorized procedures.
B. Automatic logoff is used when a workstation is inactive for a particular period of time.
C. Automatic logoff of the system occurs after a specified number of unsuccessful attempts.
D. Unsuccessful logon attempts are monitored by the security administrator.

Answer: D
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 NO: 772

Which of the following is a feature of an intrusion detection system (IDS)?

A. Gathering evidence on attack attempts
B. Identifying weaknesses in the policy definition
C. Blocking access to particular sites on the Internet
D. Preventing certain users from accessing specific servers

Answer: A
Explanation:

An IDS can gather evidence on intrusive activity such as an attack or penetration attempt. Identifying weaknesses in the policy definition is a limitation of an IDS. Choices C and D are features of firewalls, while choice B requires a manual review, and therefore is outside the functionality of an IDS.

QUESTION NO: 773

An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

A. maintenance of access logs of usage of various system resources.
B. authorization and authentication of the user prior to granting access to system resources.
C. adequate protection of stored data on servers by encryption or other means.
D. accountability system and the ability to identify any terminal accessing system resources.

Answer: B
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 NO: 774

Which of the following is the MOST effective type of antivirus software?

A. Scanners
B. Active monitors
C. integrity checkers
D. Vaccines

Answer: C
Explanation:
Integrity checkers compute a binary number on a known virus-free program that is then stored in a database file. This number is called a cyclical redundancy check (CRC). When that program is called to execute, the checker computes the CRC on the program about to be executed and compares it to the number in the database. A match means no infection; a mismatch means that a change in the program has occurred. A change in the program could mean a virus. Scanners look for sequences of bits called signatures that are typical of virus programs. They examine memory,

disk boot sectors, executables and command files for bit patterns that match a known virus. Therefore, scanners need to be updated periodically to remain effective. Active monitors interpret DOS and ROM basic input-output system (BIOS) calls, looking for virus-like actions. Active monitors can be misleading, because they cannot distinguish between a user request and a program or virus request. As a result, users are asked to confirm actions like formatting a disk or deleting a file or set of files. Vaccines are known to be good antivirus software. However, they also need to be updated periodically to remain effective.

QUESTION NO: 775

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

A. both the key used to encrypt and decrypt the data are public.
B. the key used to encrypt is private, but the key used to decrypt the data is public.
C. the key used to encrypt is public, but the key used to decrypt the data is private.
D. both the key used to encrypt and decrypt the data are private.

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

QUESTION NO: 776

The technique used to ensure security in virtual private networks (VPNs) is:

A. encapsulation.
B. wrapping.
C. transform.
D. encryption.

Answer: A
Explanation:
Encapsulation, or tunneling, is a technique used to carry the traffic of one protocol over a network that does not support that protocol directly. The original packet is wrapped in another packet. The other choices are not security techniques specific to VPNs.

QUESTION NO: 777

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:

A. encryption.
B. callback modems.
C. message authentication.
D. dedicated leased lines.

Answer: A
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 NO: 778

An internet-based attack using password sniffing can:

A. enable one party to act as if they are another party.
B. cause modification to the contents of certain transactions.
C. be used to gain access to systems containing proprietary information.
D. result in major problems with billing systems and transaction processing agreements.

Answer: C
Explanation:
Password sniffing attacks can be used to gain access to systems on which proprietary information is stored. Spoofing attacks can be used to enable one party to act as if they are another party. Data modification attacks can be used to modify the contents of certain transactions. Repudiation of transactions can cause major problems with billing systems and transaction processing agreements.

QUESTION NO: 779

Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

A. Proxy server
B. Firewall installation
C. Network administrator
D. Password implementation and administration

Answer: D
Explanation:
The most comprehensive control in this situation is password implementation and administration. While firewall installations are the primary line of defense, they cannot protect all access and, therefore, an element of risk remains. A proxy server is a type of firewall installation; thus, the same rules apply. The network administrator may serve as a control, but typically this would not be

comprehensive enough to serve on multiple and diverse systems.

QUESTION NO: 780

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. A biometric, digitalized and encrypted parameter with the customer's public key
B. A hash of the data that is transmitted and encrypted with the customer's private key
C. A hash of the data that is transmitted and encrypted with the customer's public key
D. The customer's scanned signature encrypted with the customer's public key

Answer: B
Explanation:
The calculation of a hash, or digest, of the data that are transmitted and its encryption require the public key of the client (receiver) and is called a signature of the message, or digital signature. The receiver performs the same process and then compares the received hash, once it has been decrypted with their private key, to the hash that is calculated with the received datA. If they are the same, the conclusion would be that there is integrity in the data that have arrived and the origin is authenticated. The concept of encrypting the hash with the private key of the originator provides non repudiation, as it can only be decrypted with their public key and, as the CD suggests, the private key would not be known to the recipient. Simply put, in a key-pair situation, anything that can be decrypted by a sender's public key must have been encrypted with their private key, so they must have been the sender, i.e., non repudiation. Choice C is incorrect because, if this were the case, the hash could not be decrypted by the recipient, so the benefit of non repudiation would be lost and there could be no verification that the message had not been intercepted and amended. A digital signature is created by encrypting with a private key. A person creating the signature uses their own private key, otherwise everyone would be able to create a signature with any public key. Therefore, the signature of the client is created with the client's private key, and this can be verified-by

QUESTION NO: 781

When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

A. Wiring and schematic diagram
B. Users' lists and responsibilities
C. Application lists and their details
D. Backup and recovery procedures

Answer: A

Explanation:

The wiring and schematic diagram of the network is necessary to carry out a network audit. A network audit may not be feasible if a network wiring and schematic diagram is not available. All other documents are important but not necessary.

QUESTION NO: 782

Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity and nonrepudiation by either sender or recipient?

A. The recipient uses their private key to decrypt the secret key.
B. The encrypted prehash code and the message are encrypted using a secret key.
C. The encrypted prehash code is derived mathematically from the message to be sent.
D. The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.

Answer: D

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 NO: 783

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:

A. customer over the authenticity of the hosting organization.
B. hosting organization over the authenticity of the customer.
C. customer over the confidentiality of messages from the hosting organization.
D. hosting organization over the confidentiality of messages passed to the customer.

Answer: A

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 NO: 784 CORRECT TEXT

E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

(A) sender's private key and encrypting the message using the receiver's public key.

B. sender's public key and encrypting the message using the receiver's private key.

C. receiver's private key and encrypting the message using the sender's public key.

D. receiver's public key and encrypting the message using the sender's private key.

Answer: A

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 NO: 785

An organization is considering connecting a critical PC-based system to the Internet. Which of the following would provide the BEST protection against hacking?

A. An application-level gateway
B. A remote access server
C. A proxy server
D. Port scanning

Answer: A

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 NO: 786

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?

A. Virtual private network
B. Dedicated line
C. Leased line
D. integrated services digital network

Answer: A
Explanation:
The most secure method is a virtual private network (VPN), using encryption, authentication and tunneling to allow data to travel securely from a private network to the internet. Choices B, C and D are network connectivity options that are normally too expensive to be practical for small- to medium-sized organizations.

QUESTION NO: 787

The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

A. connecting points are available in the facility to connect laptops to the network.
B. users take precautions to keep their passwords confidential.
C. terminals with password protection are located in insecure locations.
D. terminals are located within the facility in small clusters under the supervision of an administrator.

Answer: A
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 NO: 788

Which of the following functions is performed by a virtual private network (VPN)?

A. Hiding information from sniffers on the net
B. Enforcing security policies
C. Detecting misuse or mistakes
D. Regulating access

Answer: A
Explanation:
A VPN hides information from sniffers on the net using encryption. It works based on tunneling. A VPN does not analyze information packets and, therefore, cannot enforce security policies, it also does not check the content of packets, so it cannot detect misuse or mistakes. A VPN also does not perform an authentication function and, therefore, cannot regulate access.

QUESTION NO: 789

Applying a digital signature to data traveling in a network provides:

A. confidentiality and integrity.
B. security and nonrepudiation.
C. integrity and nonrepudiation.
D. confidentiality and nonrepudiation.

Answer: C
Explanation:
The process of applying a mathematical algorithm to the data that travel in the network and placing the results of this operation with the hash data is used for controlling data integrity, since any unauthorized modification to this data would result in a different hash. The application of a digital signature would accomplish the non repudiation of the delivery of the message. The term security is a broad concept and not a specific one. In addition to a hash and a digital signature, confidentiality is applied when an encryption process exists.

QUESTION NO: 790

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?

A. Customers are widely dispersed geographically, but the certificate authorities are not.
B. Customers can make their transactions from any computer or mobile device.
C. The certificate authority has several data processing subcenters to administer certificates.
D. The organization is the owner of the certificate authority.

Answer: D
Explanation:
If the certificate authority belongs to the same organization, this would generate a conflict of interest. That is, if a customer wanted to repudiate a transaction, they could allege that because of the shared interests, an unlawful agreement exists between the parties generating the certificates, if a customer wanted to repudiate a transaction, they could argue that there exists a bribery between the parties to generate the certificates, as shared interests exist. The other options are not weaknesses.

QUESTION NO: 791

Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
B. Secure Sockets Layer (SSL) mode
C. Tunnel mode with AH plus ESP
D. Triple-DES encryption mode

Answer: C
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 NO: 792

Which of the following is the MOST reliable sender authentication method?

A. Digital signatures
B. Asymmetric cryptography

C. Digital certificates
D. Message authentication code

Answer: C
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 (PKl), appearsto 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 NO: 793

Which of the following provides the GREATEST assurance of message authenticity?

A. The prehash code is derived mathematically from the message being sent.
B. The prehash code is encrypted using the sender's private key.
C. The prehash code and the message are encrypted using the secret key.
D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Answer: B
Explanation:
Encrypting the prehash code using the sender's private key provides assurance of the authenticity of the message. Mathematically deriving the prehash code provides integrity to the message. Encrypting the prehash code and the message using the secretkey provides confidentiality.

QUESTION NO: 794

Which of the following internet security threats could compromise integrity?

A. Theft of data from the client
B. Exposure of network configuration information
C. A Trojan horse browser
D. Eavesdropping on the net

Answer: C
Explanation:
Internet security threats/vulnerabilities to integrity include a Trojan horse, which could modify user data, memory and messages found in client-browser software. The other options compromise confidentiality.

QUESTION NO: 795

Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

A. The organization does not have control over encryption.
B. Messages are subjected to wire tapping.
C. Data might not reach the intended recipient.
D. The communication may not be secure.

Answer: A
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 wire tapping. Since SSL does the client authentication, only the intended recipient will receive the decrypted datA. All data sent over an encrypted SSL connection are protected with a mechanism to detect tampering, i.e., automatically determining whether data has been altered in transit.

QUESTION NO: 796

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

A. Router configuration and rules
B. Design of the internal network
C. Updates to the router system software
D. Audit testing and review techniques

Answer: A
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 NO: 797

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

A. symmetric encryption.
B. message authentication code.
C. hash function.
D. digital signature certificates.

Answer: A
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 NO: 798

The PRIMARY goal of a web site certificate is:

A. authentication of the web site that will be surfed.
B. authentication of the user who surfs through that site.
C. preventing surfing of the web site by hackers.
D. the same purpose as that of a digital certificate.

Answer: A
Explanation:
Authenticating the site to be surfed is the primary goal of a web certificate. Authentication of a user is achieved through passwords and not by a web site certificate. The site certificate does not prevent hacking nor does it authenticate a person.

QUESTION NO: 799

An IS auditor performing detailed network assessments and access control reviews should FIRST:

A. determine the points of entry.
B. evaluate users' access authorization.
C. assess users' identification and authorization.
D. evaluate the domain-controlling server configuration.

Answer: A
Explanation:
In performing detailed network assessments and access control reviews, an IS auditor should first determine the points of entry to the system and review the points of entry accordingly for appropriate controls. Evaluation of user access authorization, assessment of user identification and authorization, and evaluation of the domain-controlling server configuration are all implementation issues for appropriate controls for the points of entry.

QUESTION NO: 800

The difference between a vulnerability assessment and a penetration test is that a vulnerability assessment:

A. 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.
B. and penetration tests are different names for the same activity.
C. is executed by automated tools, whereas penetration testing is a totally manual process.
D. is executed by commercial tools, whereas penetration testing is executed by public processes.

Answer: A
Explanation:
The objective of a vulnerability assessment is to find the security holds in the computers and elements analyzed; its intent is not to damage the infrastructure. The intent of penetration testing is to imitate a hacker's activities and determine how far they could go into the network. They are not the same; they have different approaches. Vulnerability assessments and penetration testing can be executed by automated or manual tools or processes and can be executed by commercial or free tools.

QUESTION NO: 801

The most common problem in the operation of an intrusion detection system (IDS) is:

A. the detection of false positives.
B. receiving trap messages.
C. reject-error rates.
D. denial-of-service attacks.

Answer: A
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 auditorneeds 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 aregenerated 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 NO: 802

Which of the following provides nonrepudiation services for e-commerce transactions?

A. Public key infrastructure (PKI)
B. Data Encryption Standard (DES)
C. Message authentication code (MAC)
D. Personal identification number (PIN)

Answer: A
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 theperson using it; and it is linked to data in such a manner that if data are changed, the digital signature is invalidated. PKI meets these tests. The Data Encryption Standard (DES) is the most common private key cryptographic system. DES does not address nonrepudiation. A MAC is a cryptographic value calculated by passing an entire message through a cipher system. The sender attaches the MAC before transmission and the receiver recalculates the MAC and compares it to the sent MAC. If the two MACs are not equal, this indicates that the message has been altered during transmission; it has nothing to do with nonrepudiation. A PIN is a type of password, a secret number assigned to an individual that, in conjunction with some other means of identification, serves to verify the authenticity of the individual.

QUESTION NO: 803

While copying files from a floppy disk, a user introduced a virus into the network. Which of the following would MOST effectively detect the existence of the virus?

A. A scan of all floppy disks before use
B. A virus monitor on the network file server
C. Scheduled daily scans of all network drives
D. A virus monitor on the user's personal computer

Answer: C
Explanation:
Scheduled daily scans of all network drives will detect the presence of a virus after the infection has occurred. All of the other choices are controls designed to prevent a computer virus from infecting the system.

QUESTION NO: 804

Which of the following message services provides the strongest evidence that a specific action has occurred?

A. Proof of delivery
B. Nonrepudiation
C. Proof of submission
D. Message origin authentication

Answer: B
Explanation:
Nonrepudiation services provide evidence that a specific action occurred. Nonrepudiation services are similar to their weaker proof counterparts, i.e., proof of submission, proof of delivery and message origin authentication. However, nonrepudiationprovides 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 specificaction that has been completed.

QUESTION NO: 805

The PRIMARY objective of Secure Sockets Layer (SSL) is to ensure:

A. only the sender and receiver are able to encrypt/decrypt the data.
B. the sender and receiver can authenticate their respective identities.
C. the alteration of transmitted data can be detected.
D. the ability to identify the sender by generating a one-time session key.

Answer: A
Explanation:
SSL generates a session key used to encrypt/decrypt the transmitted data, thus ensuring its confidentiality. Although SSL allows the exchange of X509 certificates to provide for identification and authentication, this feature along with choices C and D are not the primary objectives.

QUESTION NO: 806

The role of the certificate authority (CA) as a third party is to:

A. provide secured communication and networking services based on certificates.
B. host a repository of certificates with the corresponding public and secret keys issued by that CA.
C. act as a trusted intermediary between two communication partners.
D. confirm the identity of the entity owning a certificate issued by that CA.

Answer: D
Explanation:
The primary activity of a CA is to issue certificates. The primary role of the CA is to check the identity of the entity owning a certificate and to confirm the integrity of any certificate it issued.

Providing a communication infrastructure is not a CA activity. The secret keys belonging to the certificates would 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 NO: 807

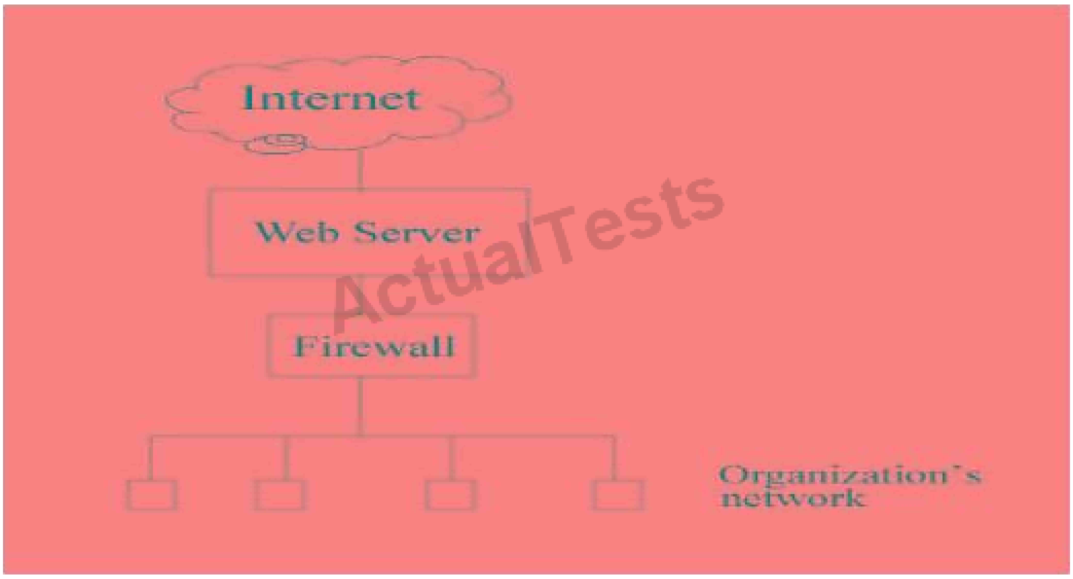
Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

A. The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
B. All personal SET certificates are stored securely in the buyer's computer.
C. The buyer is liable for any transaction involving his/her personal SET certificates.
D. The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Answer: C
Explanation:
The usual agreement between the credit card issuer and the cardholder stipulates that the cardholder assumes responsibility for any use of their personal SET certificates for e-commerce transactions. Depending upon the agreement between the merchant and the buyer's credit card issuer, the merchant will have access to the credit card number and expiration date. Secure data storage in the buyer's computer (local computer security) is not part of the SET standard. Although the buyer is not required to enter their credit card data, they will have to handle the wallet software.

QUESTION NO: 808

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

A. alert the appropriate staff.
B. create an entry in the log.
C. close firewall-2.
D. close firewall-1.

Answer: C
Explanation:
Traffic for the internal network that did not originate from the mail gateway is a sign that firewall-1 is not functioning properly. This may have been be caused by an attack from a hacker. Closing firewa!l-2 is the first thing that should be done, thus preventing damage to the internal network. After closing firewall-2, the malfunctioning of firewall-1 can be investigated. The IDS should trigger the closing of firewall-2 either automatically or by manual intervention. Between the detection by the IDS and a response from the system administrator valuable time can be lost, in which a hacker could also compromise firewall-2. An entry in the log is valuable for later analysis, but before that, the IDS should close firewall-2. If firewall-1 has already been compromised by a hacker, it might not be possible for the IDS to close it.

QUESTION NO: 809

An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

A. The data collected on attack methods
B. The information offered to outsiders on the honeypot
C. The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
D. The risk that the honeypot would be subject to a distributed denial-of-service attack

Answer: C

Explanation:

Choice C represents the organizational risk that the honeypot could be used as a point of access to launch further attacks on the enterprise's systems. Choices A and B are purposes for deploying a honeypot, not a concern. Choice D, the risk that thehoneypot would be subject to a distributed denial-of-service (DDoS) attack, is not relevant, as the honeypot is not a critical device for providing service.

QUESTION NO: 810

Which of the following should be a concern to an IS auditor reviewing a wireless network?

A. 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
B. SSID (Service Set IDentifier) broadcasting has been enabled.
C. Antivirus software has been installed in all wireless clients.
D. MAC (Media Access Control) access control filtering has been deployed.

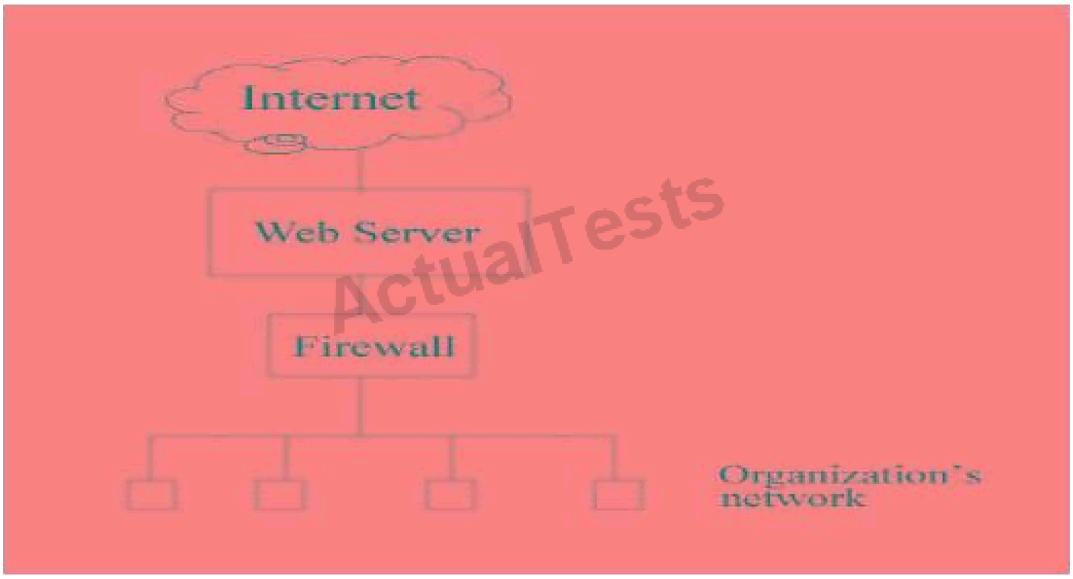
Answer: B

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 NO: 811

To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



A. Firewall and the organization's network.
B. Internet and the firewall.
C. Internet and the web server.
D. Web server and the firewall.

Answer: A

Explanation:

Attack attempts that could not be recognized by the firewall will be detected if a network-based intrusion detection system is placed between the firewall and the organization's network. A network-based intrusion detection system placed between the internet and the firewall will detect attack attempts, whether they do or do not enter the firewall.

QUESTION NO: 812

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

A. 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
B. The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
C. Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
D. Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Answer: C

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 NO: 813

An efficient use of public key infrastructure (PKI) should encrypt the:

A. entire message.
B. private key.
C. public key.
D. symmetric session key.

Answer: D

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 NO: 814

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

A. DES
B. AES
C. Triple DES
D. RSA

Answer: B

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 NO: 815

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

A. MAC (Media Access Control) address filtering
B. WPA (Wi-Fi Protected Access Protocol)
C. LEAP (Lightweight Extensible Authentication Protocol)
D. SSID (service set identifier) broadcasting

Answer: D

Explanation:

Disabling SSID broadcasting adds security by making it more difficult for unauthorized users to find the name of the access point. Disabling MAC address filtering would reduce security. Using

MAC filtering makes it more difficult to access a WLAN, because it would be necessary to catch traffic and forge the MAC address. Disabling WPA reduces security. Using WPA adds security by encrypting the traffic. Disabling LEAP reduces security. Using LEAP adds security by encrypting the wireless traffic.

QUESTION NO: 816

Which of the following is BEST suited for secure communications within a small group?

A. Key distribution center
B. Certification authority
C. Web of trust
D. Kerberos Authentication System

Answer: C
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 NO: 817

Which of the following is the MOST important action in recovering from a cyberattack?

A. Creation of an incident response team
B. Use of cybenforensic investigators
C. Execution of a business continuity plan
D. Filing an insurance claim

Answer: C
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, cyberforensics 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 thatneeds to be insured and claimed for traditional and electronic exposures.

QUESTION NO: 818

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

A. War dialing
B. Social engineering
C. War driving
D. Password cracking

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

QUESTION NO: 819

In a public key infrastructure, a registration authority:

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

Answer: A
Explanation:
A registration authority is responsible for verifying information supplied by the subject requesting a certificate, and verifies the requestor's right to request certificate attributes and that the requestor actually possesses the private key corresponding to the public key being sent. Certification authorities, not registration authorities, actually issue certificates once verification of the information has been completed; because of this, choice B is incorrect. On the other hand, the sender who has control of their private key signs the message, not the registration authority. Registering signed messages is not a task performed by registration authorities.

QUESTION NO: 820

Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

A. restricted to predefined MAC addresses.
B. encrypted using static keys.
C. encrypted using dynamic keys.
D. initiated from devices that have encrypted storage.

Answer: C
Explanation:
When using dynamic keys, the encryption key is changed frequently, thus reducing the risk of the key being compromised and the message being decrypted. Limiting the number of devices that can access the network does not address the issue of encrypting the session. Encryption with static keys-using the same key for a long period of time-risks that the key would be compromised. Encryption of the data on the connected device (laptop, PDA, etc.) addresses the confidentiality of the data on the device, not the wireless session.

QUESTION NO: 821

Which of the following provides the MOST relevant information for proactively strengthening security settings?

A. Bastion host
B. Intrusion detection system
C. Honeypot
D. Intrusion prevention system

Answer: C
Explanation:
The design of a honeypot is such that it lures the hacker and provides clues as to the hacker's methods and strategies and the resources required to address such attacks. A bastion host does not provide information about an attack. Intrusion detection systems and intrusion prevention systems are designed to detect and address an attack in progress and stop it as soon as possible. A honeypot allows the attack to continue, so as to obtain information about the hacker's strategy and methods.

QUESTION NO: 822

Over the long term, which of the following has the greatest potential to improve the security incident response process?

A. A walkthrough review of incident response procedures
B. Postevent reviews by the incident response team
C. Ongoing security training for users

D. Documenting responses to an incident

Answer: B

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 NO: 823

When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

A. Number of nonthreatening events identified as threatening
B. Attacks not being identified by the system
C. Reports/logs being produced by an automated tool
D. Legitimate traffic being blocked by the system

Answer: B

Explanation:

Attacks not being identified by the system present a higher risk, because they are unknown and no action will be taken to address the attack. Although the number of false-positives is a serious issue, the problem will be known and can be corrected. Often, IDS reports are first analyzed by an automated tool to eliminate known false-positives, which generally are not a problem. An IDS does not block any traffic.

QUESTION NO: 824

Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

A. Logic bombs
B. Phishing
C. Spyware
D. Trojan horses

Answer: D

Explanation:

Trojan horses are malicious or damaging code hidden within an authorized computer program. Hackers use Trojans to mastermind DDOS attacks that affect computers that access the same Internet site at the same moment, resulting in overloaded site servers that may no longer be able to process legitimate requests. Logic bombs are programs designed to destroy or modify data at a specific time in the future. Phishing is an attack, normally via e-mail, pretending to be an authorized person or organization requesting information. Spyware is a program that picks up information from PC drives by making copies of their contents.

QUESTION NO: 825

Validated digital signatures in an e-mail software application will:

A. help detect spam.
B. provide confidentiality.
C. add to the workload of gateway servers.
D. significantly reduce available bandwidth.

Answer: A
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 NO: 826

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

A. connectionless integrity.
B. data origin authentication.
C. antireplay service.
D. confidentiality.

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

QUESTION NO: 827

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?

A. Denial-of-service
B. Replay
C. Social engineering
D. Buffer overflow

Answer: A

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-uservulnerabilities, and buffer overflow attacks exploit poorly written code.

QUESTION NO: 828

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?

A. Port scanning
B. Back door
C. Man-in-the-middle
D. War driving

Answer: D

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 leftin software that enables an unknown entry into a system. Man-in-the-middle attacks intercept a message and either replace or modify it.

QUESTION NO: 829

Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

A. 128-bit wired equivalent privacy (WEP)
B. MAC-basedpre-sharedkey(PSK)

C. Randomly generated pre-shared key (PSKJ
D. Alphanumeric service set identifier (SSID)

Answer: C
Explanation:
A randomly generated PSK is stronger than a MAC-based PSK, because the MAC address of a computer is fixed and often accessible. WEP has been shown to be a very weak encryption technique and can be cracked within minutes. The SSID is broadcast on the wireless network in plaintext.

QUESTION NO: 830

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?

A. Reliability and quality of service (QoS)
B. Means of authentication
C. Privacy of voice transmissions
D. Confidentiality of data transmissions

Answer: A
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 NO: 831

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?

A. Heuristic (rule-based)
B. Signature-based
C. Pattern matching
D. Bayesian (statistical)

Answer: D
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 withinnormal 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 NO: 832

Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

A. Certificate revocation list (CRL)
B. Certification practice statement (CPS)
C. Certificate policy (CP)
D. PKI disclosure statement (PDS)

Answer: B
Explanation:
The CPS is the how-to part in policy-based PKI. The CRL is a list of certificates that have been revoked before their scheduled expiration date. The CP sets the requirements that are subsequently implemented by the CPS. The PDS covers critical items.such as the warranties, limitations and obligations that legally bind each party.

QUESTION NO: 833

Active radio frequency ID (RFID) tags are subject to which of the following exposures?

A. Session hijacking
B. Eavesdropping
C. Malicious code
D. Phishing

Answer: B
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 NO: 834

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?

A. Use the IP address of an existing file server or domain controller.

B. Pause the scanning every few minutes to allow thresholds to reset.
C. Conduct the scans during evening hours when no one is logged-in.
D. Use multiple scanning tools since each tool has different characteristics.

Answer: B
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.

QUESTION NO: 835

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

A. Denial-of-service
B. Man-in-the-middle
C. Key logging
D. Brute force

Answer: B
Explanation:
A man-in-the-middle attack is similar to piggybacking, in that the attacker pretends to be the legitimate destination, and then merely retransmits whatever is sent by the authorized user along with additional transactions after authentication has been accepted. A denial-of-service attack does not have a relationship to authentication. Key logging and brute force could circumvent a normal authentication but not a two-factor authentication.

QUESTION NO: 836

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

A. digitally signing all e-mail messages.
B. encrypting all e-mail messages.
C. compressing all e-mail messages.
D. password protecting all e-mail messages.

Answer: A
Explanation:
By digitally signing all e-mail messages, the receiver will be able to validate the authenticity of the

sender. Encrypting all e-mail messages would ensure that only the intended recipient will be able to open the message; however, it would not ensure the authenticity of the sender. Compressing all e-mail messages would reduce the size of the message, but would not ensure the authenticity. Password protecting all e-mail messages would ensure that only those who have the password would be able toopen the message; however, it would not ensure the authenticity of the sender.

QUESTION NO: 837

Sending a message and a message hash encrypted by the sender's private key will ensure:

A. authenticity and integrity.
B. authenticity and privacy.
C. integrity and privacy.
D. privacy and nonrepudiation.

Answer: A
Explanation:
If the sender sends both a message and a message hash encrypted by its private key, then the receiver can apply the sender's public key to the hash and get the message hash. The receiver can apply the hashing algorithm to the message received and generate a hash. By matching the generated hash with the one received, the receiver is ensured that the message has been sent by the specific sender, i.e., authenticity, and that the message has not been changed enroute. Authenticity and privacy will beensured by first using the sender's private key and then the receiver's public key to encrypt the message. Privacy and integrity can be ensured by using the receiver's public key to encrypt the message and sending a message hash/digest. Only nonrepudiation can be ensured by using the sender's private key to encrypt the message. The sender's public key, available to anyone, can decrypt a message; thus, it does not ensure privacy.

QUESTION NO: 838

Which of the following is a passive attack to a network?

A. Message modification
B. Masquerading
C. Denial of service
D. Traffic analysis

Answer: D
Explanation:
The intruder determines the nature of the flow of traffic (traffic analysis) between defined hosts and is able to guess the type of communication taking place. Message modification involves the capturing of a message and making unauthorized changes or deletions, changing the sequence or

delaying transmission of captured messages. Masquerading is an active attack in which the intruder presents an identity other than the original identity. Denial of service occurs when a computer connected to theInternet is flooded with data and/or requests that must be processed.

QUESTION NO: 839

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 nonupgradeabie access points. Which of the following would BEST justify the IS auditor's recommendation?

A. The new access points with stronger security are affordable.
B. The old access points are poorer in terms of performance.
C. The organization's security would be as strong as its weakest points.
D. The new access points are easier to manage.

Answer: C
Explanation:
The old access points should be discarded and replaced with products having strong security; otherwise, they will leave security holes open for attackers and thus make the entire network as weak as they are. Affordability is not the auditor's major concern. Performance is not as important as security in this situation. Product manageability is not the IS auditor's concern.

QUESTION NO: 840

An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

A. encrypting the hash of the newsletter using the advisor's private key.
B. encrypting the hash of the newsletter using the advisor's public key.
C. digitally signing the document using the advisor's private key.
D. encrypting the newsletter using the advisor's private key.

Answer: A
Explanation:
There is no attempt on the part of the investment advisor to prove their identity or to keep the newsletter confidential. The objective is to assure the receivers that it came to them without any modification, i.e., it has message integrity. Choice Ais correct because the hash is encrypted using the advisor's private key. The recipients can open the newsletter, recompute the hash and decrypt the received hash using the advisor's public key. If the two hashes are equal, the newsletter was not modified in transit. Choice B is not feasible, for no one other than the investment advisor can open it. Choice C addresses sender authentication but not message integrity. Choice D addresses confidentiality, but not message integrity, because anyone can obtain the investment advisor's

public key, decrypt the newsletter, modify it and send it to others. The interceptor will not be able to use the advisor's private key, because they do not have it. Anything encrypted using the interceptor's privatekey can be decrypted by the receiver only by using their public key.

QUESTION NO: 841

An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

A. reduces the risk of unauthorized access to the network.
B. is not suitable for small networks.
C. automatically provides an IP address to anyone.
D. increases the risks associated with Wireless Encryption Protocol (WEP).

Answer: A
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 NO: 842

A virtual private network (VPN) provides data confidentiality by using:

A. Secure Sockets Layer (SSL)
B. Tunnelling
C. Digital signatures
D. Phishing

Answer: B
Explanation:
VPNs secure data in transit by encapsulating traffic, a process known as tunnelling. SSL is a symmetric method of encryption between a server and a browser. Digital signatures are not used in the VPN process, while phishing is a form of a social engineering attack.

QUESTION NO: 843

In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

A. common gateway interface (CGI) scripts.
B. enterprise Java beans (EJBs).
C. applets.
D. web services.

Answer: A
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 requiresknowledge of the parameters and expected return values.

QUESTION NO: 844

An IS auditor reviewing access controls for a client-server environment should FIRST:

A. evaluate the encryption technique.
B. identify the network access points.
C. review the identity management system.
D. review the application level access controls.

Answer: B
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 accesspoints 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 NO: 845

To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

A. the source routing field is enabled.
B. it has a broadcast address in the destination field.
C. a reset flag (RST) is turned on for the TCP connection.

D. dynamic routing is used instead of static routing.

Answer: A

Explanation:

IP spoofing takes advantage of the source-routing option in the IP protocol. With this option enabled, an attacker can insert a spoofed source IP address. The packet will travel the network according to the information within the source-routing field, bypassing the logic in each router, including dynamic and static routing (choice D). Choices B and C do not have any relation to IP spoofing attacks. If a packet has a broadcast destination address (choice B), it will be sent to all addresses in the subnet. Turning on the reset flag (RST) (choice C) is part of the normal procedure to end a TCP connection.

QUESTION NO: 846

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

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

Answer: D

Explanation:

An intrusion detection system (IDS) cannot detect attacks within encrypted traffic, and it would be a concern if someone was misinformed and thought that the IDS could detect attacks in encrypted traffic. An organization can place sensors outside of the firewall to detect attacks. These sensors are placed in highly sensitive areas and on extranets. Causing many false alarms is normal for a behavior-based IDS, and should not be a matter of concern. Being weak against new types of attacks is also expected from a signature-based IDS, because it can only recognize attacks that have been previously identified.

QUESTION NO: 847

Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

A. Encrypts the information transmitted over the network
B. Makes other users' certificates available to applications
C. Facilitates the implementation of a password policy
D. Stores certificate revocation lists (CRLs)

Answer: B

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 (PKl).

QUESTION NO: 848

An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

A. provides authenticity.
B. is faster than asymmetric encryption.
C. can cause key management to be difficult.
D. requires a relatively simple algorithm.

Answer: C

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 NO: 849

Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

A. A remote access server
B. A proxy server
C. A personal firewall
D. A password-generating token

Answer: C

Explanation:

A personal firewall is the best way to protect against hacking, because it can be defined with rules that describe the type of user or connection that is or is not permitted. A remote access server can be mapped or scanned from the Internet, creating security exposures. Proxy servers can provide protection based on the IP address and ports; however, an individual would need to have in-depth knowledge to do this, and applications can use different ports for the different sections of their program. A password-generating token may help to encrypt the session but does not protect a computer against hacking.

QUESTION NO: 850

When installing an intrusion detection system (IDS), which of the following is MOST important?

A. Properly locating it in the network architecture
B. Preventing denial-of-service (DoS) attacks
C. Identifying messages that need to be quarantined
D. Minimizing the rejection errors

Answer: A
Explanation:
Proper location of an intrusion detection system (IDS) in the network is the most important decision during installation. A poorly located IDS could leave key areas of the network unprotected. Choices B, C and D are concerns during the configuration of an IDS, but if the IDS is not placed correctly, none of them would be adequately addressed.

QUESTION NO: 851

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?

A. Nonrepudiation
B. Encryption
C. Authentication
D. Integrity

Answer: A
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.

QUESTION NO: 852

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

A. Digital signature
B. Digital certificate
C. Online Certificate Status Protocol
D. Private key cryptosystem

Answer: D

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 NO: 853

To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

A. access control servers.
B. session border controllers.
C. backbone gateways.
D. intrusion detection system (IDS).

Answer: B

Explanation:

Session border controllers enhance the security in the access network and in the core. In the access network, they hide a user's real address and provide a managed public address. This public address can be monitored, minimizing the opportunities forscanning and denial-of-service (DoS) attacks. Session border controllers permit access to clients behind firewalls while maintaining the firewall's effectiveness. In the core, session border controllers protect the users and the network. They hide network topology and users' real addresses. They can also monitor bandwidth and quality of service. Securing the access control server, backbone gateways and intrusion detection systems (IDSs) does not effectively protect against DoS attacks.

QUESTION NO: 854

Which of the following attacks targets the Secure Sockets Layer (SSL)?

A. Man-in-the middle
B. Dictionary
C. Password sniffing
D. Phishing

Answer: A

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 byfalsely claiming to be a trusted person or enterprise.

QUESTION NO: 855

Which of the following potentially blocks hacking attempts?

A. intrusion detection system
B. Honeypot system
C. Intrusion prevention system
D. Network security scanner

Answer: C
Explanation:
An intrusion prevention system (IPS) is deployed as an in-line device that can detect and block hacking attempts. An intrusion detection system (IDS) normally is deployed in sniffing mode and can detect intrusion attempts, but cannot effectively stopthem. A honeypot solution traps the intruders to explore a simulated target. A network security scanner scans for the vulnerabilities, but it will not stop the intrusion.

QUESTION NO: 856

A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

A. Dump the volatile storage data to a disk.
B. Run the server in a fail-safe mode.
C. Disconnect the web server from the network.
D. Shut down the web server.

Answer: C
Explanation:
The first action is to disconnect the web server from the network to contain the damage and prevent more actions by the attacker. Dumping the volatile storage data to a disk may be used at the investigation stage but does not contain an attack in progress. To run the server in a fail-safe mode, the server needs to be shut down. Shutting down the server could potentially erase information that might be needed for a forensic investigation or to develop a strategy to prevent future similar attacks.

QUESTION NO: 857

To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

A. Secure Shell (SSH-2) tunnel for the duration of the problem.
B. two-factor authentication mechanism for network access.
C. dial-in access.
D. virtual private network (VPN) account for the duration of the vendor support contract.

Answer: A
Explanation:
For granting temporary access to the network, a Secure Shell (SSH-2) tunnel is the best approach. It has auditing features and allows restriction to specific access points. Choices B, C and D all give full access to the internal network. Two-factor authentication and virtual private network (VPN) provide access to the entire network and are suitable for dedicated users. Dial-in access would need to be closely monitored or reinforced with another mechanism to ensure authentication to achieve thesame level of security as SSH-2.

QUESTION NO: 858

What is the BEST approach to mitigate the risk of a phishing attack?

A. implement an intrusion detection system (IDS)
B. Assess web site security
C. Strong authentication
D. User education

Answer: D
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 masqueradingas 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 pagesand e-mail.

QUESTION NO: 859

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

A. date and time stamp of the message.
B. identity of the originating computer.

C. confidentiality of the message's content.
D. authenticity of the sender.

Answer: D
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 NO: 860

The BEST filter rule for protecting a network from being used as an amplifier in a denial of service (DoS) attack is to deny all:

A. outgoing traffic with IP source addresses externa! to the network.
B. incoming traffic with discernible spoofed IP source addresses.
C. incoming traffic with IP options set.
D. incoming traffic to critical hosts.

Answer: A
Explanation:
Outgoing traffic with an IP source address different than the IP range in the network is invalid, in most of the cases, it signals a DoS attack originated by an internal user or by a previously compromised internal machine; in both cases, applying this filter will stop the attack.

QUESTION NO: 861

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?

A. Antivirus software
B. Hardening the servers
C. Screening routers
D. Honeypots

Answer: D
Explanation:
Honeypots can collect data on precursors of attacks. Since they serve no business function, honeypots are hosts that have no authorized users other than the honeypot administrators. All activity directed at them is considered suspicious. Attackers will scan and attack honeypots, giving administrators data on new trends and attack tools, particularly malicious code. However, honeypots are a supplement to, not a replacement for, properly securing networks, systems and applications. If honeypots are to be used by an organization, qualified incident handlers and

intrusion detection analysts should manage them. The other choices do not provide indications of potential attacks.

QUESTION NO: 862

A company has decided to implement an electronic signature scheme based on public key infrastructure. The user's private key will be stored on the computer's hard drive and protected by a password. The MOST significant risk of this approach is:

A. use of the user's electronic signature by another person if the password is compromised.
B. forgery by using another user's private key to sign a message with an electronic signature.
C. impersonation of a user by substitution of the user's public key with another person's public key.
D. forgery by substitution of another person's private key on the computer.

Answer: A
Explanation:
The user's digital signature is only protected by a password. Compromise of the password would enable access to the signature. This is the most significant risk. Choice B would require subversion of the public key infrastructure mechanism, which is very difficult and least likely. Choice C would require that the message appear to have come from a different person and therefore the true user's credentials would not be forged. Choice D has the same consequence as choice C.

QUESTION NO: 863

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?

A. The tools used to conduct the test
B. Certifications held by the IS auditor
C. Permission from the data owner of the server
D. An intrusion detection system (IDS) is enabled

Answer: C
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 NO: 864

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?

A. Server is a member of a workgroup and not part of the server domain
B. Guest account is enabled on the server
C. Recently, 100 users were created in the server
D. Audit logs are not enabled for the server

Answer: D
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 apoor 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 NO: 865

Which of the following would be the GREATEST cause for concern when data are sent over the Internet using HTTPS protocol?

A. Presence of spyware in one of the ends
B. The use of a traffic sniffing tool
C. The implementation of an RSA-compliant solution
D. A symmetric cryptography is used for transmitting data

Answer: A
Explanation:
Encryption using secure sockets layer/transport layer security (SSL/TLS) tunnels makes it difficult to intercept data in transit, but when spyware is running on an end user's computer, data are collected before encryption takes place. The other choices are related to encrypting the traffic, but the presence of spyware in one of the ends captures the data before encryption takes place.

QUESTION NO: 866

A firewall is being deployed at a new location. Which of the following is the MOST important factor in ensuring a successful deployment?

A. Reviewing logs frequently
B. Testing and validating the rules
C. Training a local administrator at the new location
D. Sharing firewall administrative duties

Answer: B
Explanation:

A mistake in the rule set can render a firewall insecure. Therefore, testing and validating the rules is the most important factor in ensuring a successful deployment. A regular review of log files would not start until the deployment has been completed. Training a local administrator may not be necessary if the firewalls are managed from a central location. Having multiple administrators is a good idea, but not the most important.

QUESTION NO: 867

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?

A. SSL encryption
B. Two-factor authentication
C. Encrypted session cookies
D. IP address verification

Answer: A
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.

QUESTION NO: 868

What is the MOST prevalent security risk when an organization implements remote virtual private network (VPN) access to its network?

A. Malicious code could be spread across the network
B. VPN logon could be spoofed
C. Traffic could be sniffed and decrypted
D. VPN gateway could be compromised

Answer: A
Explanation:
VPN is a mature technology; VPN devices are hard to break. However, when remote access is enabled, malicious code in a remote client could spread to the organization's network. Though choices B, C and D are security risks, VPN technology largely mitigates these risks.

QUESTION NO: 869

The use of digital signatures:

A. requires the use of a one-time password generator.
B. provides encryption to a message.
C. validates the source of a message.
D. ensures message confidentiality.

Answer: C
Explanation:
The use of a digital signature verifies the identity of the sender, but does not encrypt the whole message, and hence is not enough to ensure confidentiality. A one-time password generator is an option, but is not a requirement for using digital signatures.

QUESTION NO: 870

The FIRST step in a successful attack to a system would be:

A. gathering information.
B. gaining access.
C. denying services.
D. evading detection.

Answer: A
Explanation:
Successful attacks start by gathering information about the target system. This is done in advance so that the attacker gets to know the target systems and their vulnerabilities. All of the other choices are based on the information gathered.

QUESTION NO: 871

The sender of a public key would be authenticated by a:

A. certificate authority,
B. digital signature.
C. digital certificate.
D. registration authority.

Answer: C
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 NO: 872

An IS auditor finds that conference rooms have active network ports. Which of the

following is MOST important to ensure?

A. The corporate network is using an intrusion prevention system (IPS)
B. This part of the network is isolated from the corporate network
C. A single sign-on has been implemented in the corporate network
D. Antivirus software is in place to protect the corporate network

Answer: B
Explanation:
If the conference rooms have access to the corporate network, unauthorized users may be able to connect to the corporate network; therefore, both networks should be isolated either via a firewall or being physically separated. An I PS would detect possible attacks, but only after they have occurred. A single sign-on would ease authentication management. Antivirus software would reduce the impact of possible viruses; however, unauthorized users would still be able to access the corporate network, which is the biggest risk.

QUESTION NO: 873

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?

A. Using virtual private network (VPN) tunnels for data transfer
B. Enabling data encryption within the application
C. Auditing the access control to the network
D. Logging all changes to access lists

Answer: A
Explanation:
The best way to ensure confidentiality and integrity of data is to encrypt it using virtual private network (VPN) tunnels. This is the most common and convenient way to encrypt the data traveling over the network. Data encryption within the application is less efficient than VPN. The other options are good practices, but they do not directly prevent the loss of data Integrity and confidentiality during communication through a network.

QUESTION NO: 874

When conducting a penetration test of an IT system, an organization should be MOST

concerned with:

A. the confidentiality of the report.
B. finding all possible weaknesses on the system.
C. restoring all systems to the original state.
D. logging all changes made to the production system.

Answer: C
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 NO: 875

Which of the following penetration tests would MOST effectively evaluate incident

handling and response capabilities of an organization?

A. Targeted testing
B. External testing
C. internal testing
D. Double-blind testing

Answer: D
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 NO: 876

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?

A. Personal firewall

B. Antivirus programs
C. Intrusion detection system (IDS)
D. Virtual local area network (VLAN) configuration

Answer: C
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 VI_AN configurations would be later in the line of defense.

QUESTION NO: 877

In wireless communication, which of the following controls allows the device receiving

the communications to verify that the received communications have not been altered in transit?

A. Device authentication and data origin authentication
B. Wireless intrusion detection (IDS) and prevention systems (IPS)
C. The use of cryptographic hashes
D. Packet headers and trailers

Answer: C
Explanation:
Calculating cryptographic hashes for wireless communications allows the device receiving the communications to verify that the received communications have not been altered in transit. This prevents masquerading and message modification attacks. Device authentication and data origin authentication is not the correct answer since authenticating wireless endpoints to each other prevents man-in-the-middle attacks and masquerading. Wireless iDS/lPSs is not the correct answer since wireless IDS/lPSshave the ability to detect misconfigured devices and rogue devices, and detect and possibly stop certain types of attacks. Packet headers and trailers alone do not ensure that the content has not been altered.

QUESTION NO: 878

An organization is planning to replace its wired networks with wireless networks. Which

of the following would BEST secure the wireless network from unauthorized access?

A. Implement Wired Equivalent Privacy (WEP)
B. Permit access to only authorized Media Access Control (MAC) addresses
C. Disable open broadcast of service set identifiers (SSID)
D. Implement Wi-Fi Protected Access (WPA) 2

Answer: D

Explanation:

Wi-Fi Protected Access (WPA) 2 implements most of the requirements of the IEEE 802.11i standard. The Advanced Encryption Standard (AESJ used in WPA2 provides better security. Also, WPA2 supports both the Extensible Authentication Protocol and the preshared secret key authentication model. Implementing Wired Equivalent Privacy (WEP) is incorrect since it can be cracked within minutes. WEP uses a static key which has to be communicated to all authorized users, thus management is difficult. Also, there is a greater vulnerability if the static key is not changed at regular intervals. The practice of allowing access based on Media Access Control (MAC) is not a solution since MAC addresses can be spoofed by attackers to gain access to the network. Disabling open broadcast of service set identifiers (SSID) is not the correct answer as they cannot handle access control.

QUESTION NO: 879

An IS auditor is reviewing a software-based firewall configuration. Which of the following

represents the GREATEST vulnerability? The firewall software:

A. is configured with an implicit deny rule as the last rule in the rule base.
B. is installed on an operating system with default settings.
C. has been configured with rules permitting or denying access to systems or networks.
D. is configured as a virtual private network (VPN) endpoint.

Answer: B

Explanation:

Default settings are often published and provide an intruder with predictable configuration information, which allows easier system compromise. To mitigate this risk, firewall software should be installed on a system using a hardened operating system that has limited functionality, providing only the services necessary to support the firewall software. Choices A, C and D are normal or best practices for firewall configurations.

QUESTION NO: 880

The GREATEST risk posed by an improperly implemented intrusion prevention system (IPS) is:

A. that there will be too many alerts for system administrators to verify.
B. decreased network performance due to IPS traffic.
C. the blocking of critical systems or services due to false triggers.
D. reliance on specialized expertise within the IT organization.

Answer: C

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 maybiock 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 NO: 881

The MOST effective control for reducing the risk related to phishing is:

A. centralized monitoring of systems.
B. including signatures for phishing in antivirus software.
C. publishing the policy on antiphishing on the intranet.
D. security training for all users.

Answer: D
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 NO: 882

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

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

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

QUESTION NO: 883

When using a digital signature, the message digest is computed:

A. only by the sender.
B. only by the receiver.
C. by both the sender and the receiver.
D. by the certificate authority (CA).

Answer: C
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 NO: 884

Which of the following would effectively verify the originator of a transaction?

A. Using a secret password between the originator and the receiver
B. Encrypting the transaction with the receiver's public key
C. Using a portable document format (PDF) to encapsulate transaction content
D. Digitally signing the transaction with the source's private key

Answer: D
Explanation:
A digital signature is an electronic identification of a person, created by using a public key algorithm, to verify to a recipient the identity of the source of a transaction and the integrity of its content. Since they are a 'shared secret' between the user and the system itself, passwords are considered a weaker means of authentication. Encrypting the transaction with the recipient's public key will provide confidentiality for the information, while using a portable document format(PDF) will probe the integrity of the content but not necessarily authorship.

QUESTION NO: 885

A perpetrator looking to gain access to and gather information about encrypted data

being transmitted over the network would use:

A. eavesdropping.
B. spoofing.
C. traffic analysis.

D. masquerading.

Answer: C

Explanation:

In traffic analysis, which is a passive attack, an intruder determines the nature of the traffic flow between defined hosts and through an analysis of session length, frequency and message length, and the intruder is able to guess the type of communication taking place. This typically is used when messages are encrypted and eavesdropping would not yield any meaningful results, in eavesdropping, which also is a passive attack, the intruder gathers the information flowing through the network withthe intent of acquiring and releasing message contents for personal analysis or for third parties. Spoofing and masquerading are active attacks, in spoofing, a user receives an e-mail that appears to have originated from one source when it actually was sent from another source. In masquerading, the intruder presents an identity other than the original identity.

QUESTION NO: 886

Upon receipt of the initial signed digital certificate the user will decrypt the certificate

with the public key of the:

A. registration authority (RA).
B. certificate authority (CA).
C. certificate repository.
D. receiver.

Answer: B

Explanation:

A certificate authority (CA) is a network authority that issues and manages security credentials and public keys for message encryption. As a part of the public key infrastructure, a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate. The CA signs the certificate with its private key for distribution to the user. Upon receipt, the user will decrypt the certificate with the CA's public key.

QUESTION NO: 887

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?

A. Review and, where necessary, upgrade firewall capabilities
B. Install modems to allow remote maintenance support access

C. Create a physically distinct network to handle VoIP traffic
D. Redirect all VoIP traffic to allow clear text logging of authentication credentials

Answer: A
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 virtualLANS (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 in crease latency since this will adversely impact VoIP quality.

QUESTION NO: 888

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

A. Statistical-based
B. Signature-based
C. Neural network
D. Host-based

Answer: A
Explanation:
A statistical-based IDS relies on a definition of known and expected behavior of systems. Since normal network activity may at times include unexpected behavior (e.g., a sudden massive download by multiple users), these activities will be flagged as suspicious. A signature-based IDS is limited to its predefined set of detection rules, just like a virus scanner. A neural network combines the previous two IDSs to create a hybrid and better system. Host-based is another classification of IDS. Any of the three IDSs above may be host- or network-based.

QUESTION NO: 889

When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

A. hardware is protected against power surges.
B. integrity is maintained if the main power is interrupted.

C. immediate power will be available if the main power is lost.
D. hardware is protected against long-term power fluctuations.

Answer: A

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 NO: 890

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

A. Halongas
B. Wet-pipe sprinklers
C. Dry-pipe sprinklers
D. Carbon dioxide gas

Answer: C

Explanation:

Water sprinklers, with an automatic power shutoff system, are accepted as efficient because they can be set to automatic release without threat to life, and water is environmentally friendly. Sprinklers must be dry-pipe to prevent the risk of leakage. Halon is efficient and effective as it does not threaten human life and, therefore, can be set to automatic release, but it is environmentally damaging and very expensive. Water is an acceptable medium but the pipes should be empty to avoid leakage, so a full system is not a viable option. Carbon dioxide is accepted as an environmentally acceptable gas, but it is less efficient because it cannot be set to automatic release in a staffed site since it threatens life.

QUESTION NO: 891

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

A. Power line conditioners
B. Surge protective devices
C. Alternative power supplies
D. Interruptible power supplies

Answer: A

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 NO: 892

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 ofthe following should be given the HIGHEST priority in the auditor's report?

A. The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
B. Both fire suppression systems present a risk of suffocation when used in a closed room.
C. The CO2 extinguisher should be removed, because CO2 is ineffective for suppressing fires involving solid combustibles (paper).
D. The documentation binders should be removed from the equipment room to reduce potential risks.

Answer: B
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 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 andpaper). Although not of highest priority, removal of the documentation would probably reduce some of the risks.

QUESTION NO: 893

Which of the following would be BEST prevented by a raised floor in the computer machine room?

A. Damage of wires around computers and servers
B. A power failure from static electricity
C. Shocks from earthquakes
D. Water flood damage.

Answer: A
Explanation:
The primary reason for having a raised floor is to enable power cables and data cables to be

installed underneath the floor. This eliminates the safety and damage risks posed when cables are placed in a spaghetti-like fashion on an open floor. Staticelectricity should be avoided in the machine room; therefore, measures such as specially manufactured carpet or shoes would be more appropriate for static prevention than a raised floor. Raised floors do not address shocks from earthquakes. To address earthquakes, anti-seismic architecture would be required to establish a quake-resistant structural framework. Computer equipment needs to be protected against water. However, a raised floor would not prevent damage to the machines in the event of overhead water pipe leakage.

QUESTION NO: 894

A penetration test performed as part of evaluating network security:

A. provides assurance that all vulnerabilities are discovered.
B. should be performed without warning the organization's management.
C. exploits the existing vulnerabilities to gain unauthorized access.
D. would not damage the information assets when performed at network perimeters.

Answer: C
Explanation:
Penetration tests are an effective method of identifying real-time risks to an information processing environment. They attempt to break into a live site in order to gain unauthorized access to a system. They do have the potential for damaging information assets or misusing information because they mimic an experienced hacker attacking a live system. On the other hand, penetration tests do not provide assurance that all vulnerabilities are discovered because they are based on a limited number of procedures. Management should provide consent for the test to avoid false alarms to IT personnel or to law enforcement bodies.

QUESTION NO: 895

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?

A. Users should not leave tokens where they could be stolen
B. Users must never keep the token in the same bag as their laptop computer
C. Users should select a PIN that is completely random, with no repeating digits
D. Users should never write down their PIN

Answer: D
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 with out the PIN; one cannot work without the other. The PIN does not need to be random as long as it is secret.

QUESTION NO: 896

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

A. Wet-pipe sprinkler system
B. Dry-pipe sprinkler system
C. FM-200system
D. Carbon dioxide-based fire extinguishers

Answer: C
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 NO: 897

During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

A. enrollment.
B. identification.
C. verification.
D. storage.

Answer: A
Explanation:
The users of a biometrics device must first be enrolled in the device. The device captures a physical or behavioral image of the human, identifies the unique features and uses an algorithm to convert them into a string of numbers stored as a template to be used in the matching processes.

QUESTION NO: 898

An accuracy measure for a biometric system is:

A. system response time.
B. registration time.
C. input file size.
D. false-acceptance rate.

Answer: D
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 NO: 899

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

A. Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
B. The contingency plan for the organization cannot effectively test controlled access practices.
C. Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
D. Removing access for those who are no longer authorized is complex.

Answer: A
Explanation:
The concept of piggybacking compromises all physical control established. Choice B would be of minimal concern in a disaster recovery environment. Items in choice C are not easily duplicated. Regarding choice D, while technology is constantly changing, card keys have existed for some time and appear to be a viable option for the foreseeable future.

QUESTION NO: 900

An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

A. False-acceptance rate (FAR)
B. Equal-error rate (EER)
C. False-rejection rate (FRR)
D. False-identification rate (FIR)

Answer: A
Explanation:
FAR is the frequency of accepting an unauthorized person as authorized, thereby granting access

when it should be denied, in an organization with high security requirements, user annoyance with a higher FRR is less important, since it is better to deny access to an authorized individual than to grant access to an unauthorized individual. EER is the point where the FAR equals the FRR; therefore, it does not minimize the FAR. FIR is the probability that an authorized person is identified, but is assigned a false ID.

QUESTION NO: 901

The MOST effective control for addressing the risk of piggybacking is:

A. a single entry point with a receptionist.
B. the use of smart cards.
C. a biometric door lock.
D. a deadman door.

Answer: D
Explanation:
Deadman doors are a system of using a pair of (two) doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding areA. This reduces the risk of an unauthorized person following an authorized person through a secured entry (piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

QUESTION NO: 902

The BEST overall quantitative measure of the performance of biometric control devices is:

A. false-rejection rate.
B. false-acceptance rate.
C. equal-error rate.
D. estimated-error rate.

Answer: C
Explanation:
A low equal-error rate (EER) is a combination of a low false-rejection rate and a low false-acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false-rejection and false-acceptance rates are equal. A low EERis the measure of the more effective biometrics control device. Low false-rejection rates or low false-acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is nonexistent and therefore irrelevant.

QUESTION NO: 903

Which of the following is the MOST effective control over visitor access to a data center?

A. Visitors are escorted.
B. Visitor badges are required.
C. Visitors sign in.
D. Visitors are spot-checked by operators.

Answer: A

Explanation:

Escorting visitors will provide the best assurance that visitors have permission to access the data processing facility. Choices B and C are not reliable controls. Choice D is incorrect because visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

QUESTION NO: 904

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

A. Replay
B. Brute force
C. Cryptographic
D. Mimic

Answer: A

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 NO: 905

A firm is considering using biometric fingerprint identification on all PCs that access critical datA. This requires:

A. that a registration process is executed for all accredited PC users.
B. the full elimination of the risk of a false acceptance.
C. the usage of the fingerprint reader be accessed by a separate password.
D. assurance that it will be impossible to gain unauthorized access to critical data.

Answer: A

Explanation:

The fingerprints of accredited users need to be read, identified and recorded, i.e., registered, before a user may operate the system from the screened PCs. Choice B is incorrect, as the false-acceptance risk of a biometric device may be optimized, but will never be zero because this would imply an unacceptably high risk of false rejection. Choice C is incorrect, as the fingerprint device reads the token (the user's fingerprint) and does not need to be protected in itself by a password. Choice Dis incorrect because the usage of biometric protection on PCs does not guarantee that other potential security weaknesses in the system may not be exploited to access protected data.

QUESTION NO: 906

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

A. Palm scan
B. Face recognition
C. Retina scan
D. Hand geometry

Answer: C

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 scannerwhere 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 lackuniqueness in the geometry datA. In face biometrics, a reader analyzes the images captured for general facial characteristics. Though considered a natural and friendly biometric, the main disadvantage of face recognition is the lack of uniqueness, which means that people looking alike can fool the device.

QUESTION NO: 907

The MOST likely explanation for a successful social engineering attack is:

A. that computers make logic errors.
B. that people make judgment errors.
C. the computer knowledge of the attackers.
D. the technological sophistication of the attack method.

Answer: B

Explanation:

Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

QUESTION NO: 908

The purpose of a deadman door controlling access to a computer facility is primarily to:

A. prevent piggybacking.
B. prevent toxic gases from entering the data center.
C. starve a fire of oxygen.
D. prevent an excessively rapid entry to, or exit from, the facility.

Answer: A

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 NO: 909

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

A. Smart card
B. Password
C. Photo identification
D. iris scan

Answer: D

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 NO: 910

A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

A. Badge readers are installed in locations where tampering would be noticed
B. The computer that controls the badge system is backed up frequently
C. A process for promptly deactivating lost or stolen badges exists
D. All badge entry attempts are logged

Answer: C
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 NO: 911

Which of the following physical access controls effectively reduces the risk of piggybacking?

A. Biometric door locks
B. Combination door locks
C. Deadman doors
D. Bolting door locks

Answer: C
Explanation:
Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding areA. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint or signature activate biometric door locks; however, they do not prevent or reduce the risk of piggybacking.
Combination door locks, also known as cipher locks, use a numeric key pad or dial to gain entry.
They do notprevent 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 NO: 912

The MOST effective biometric control system is the one:

A. which has the highest equal-error rate (EER).
B. which has the lowest EER.

C. for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
D. for which the FRR is equal to the failure-to-enroll rate (FER).

Answer: B
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 highestEER 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 NO: 913

Which of the following is the BEST way to satisfy a two-factor user authentication?

A. A smart card requiring the user's PIN
B. User ID along with password
C. Iris scanning plus fingerprint scanning
D. A magnetic card requiring the user's PIN

Answer: A
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.

QUESTION NO: 914

What should an organization do before providing an external agency physical access to its

information processing facilities (IPFs)?

A. The processes of the external agency should be subjected to an IS audit by an independent agency.
B. Employees of the external agency should be trained on the security procedures of the organization.
C. Any access by an external agency should be limited to the demilitarized zone (DMZ).
D. The organization should conduct a risk assessment and design and implement appropriate controls.

Answer: D
Explanation:

Physical access of information processing facilities (IPFs) by an external agency introduces additional threats into an organization. Therefore, a risk assessment should be conducted and controls designed accordingly. The processes of the external agency are not of concern here. It is the agency's interaction with the organization that needs to be protected. Auditing their processes would not be relevant in this scenario. Training the employees of the external agency may be one control procedure, but could be performed after access has been granted. Sometimes an external agency may require access to the processing facilities beyond the demilitarized zone (DMZ). For example, an agency which undertakes maintenance of servers may require access to the main server room. Restricting access within the DMZ will not serve the purpose.

QUESTION NO: 915

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

A. nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
B. access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
C. card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
D. the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Answer: A
Explanation:
Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequateto trust unknown external people by allowing them to write down their alleged name without proof, e.g., identity card, driver's license. Choice B is not a concern because if the name and address of the organization was written on the card, a malicious finder could use the card to enter the organization's premises. Separating card issuance from technical rights management is a method to ensure a proper segregation of duties so that no single person can produce a functioning card for a restrictedarea within the organization's premises. Choices B and C are good practices, not concerns. Choice D may be a concern, but not as important since a system failure of the card programming device would normally not mean that the readers do not functionanymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

QUESTION NO: 916

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

A. Overwriting the tapes
B. initializing the tape labels
C. Degaussing the tapes
D. Erasing the tapes

Answer: C
Explanation:
The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

QUESTION NO: 917

Which of the following is the MOST important objective of data protection?

A. identifying persons who need access to information
B. Ensuring the integrity of information
C. Denying or authorizing access to the IS system
D. Monitoring logical accesses

Answer: B
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 NO: 918

Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?

A. Processing power
B. Volume of data
C. Key distribution
D. Complexity of the algorithm

Answer: C
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 asymmetrictechniques, 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.

QUESTION NO: 919

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?

A. Rewrite the hard disk with random Os and Is.
B. Low-level format the hard disk.
C. Demagnetize the hard disk.
D. Physically destroy the hard disk.

Answer: D
Explanation:
Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical, because the hard disk is damaged. Demagnetizing is an inefficient procedure, because it requires specialized and expensive equipment to be fully effective.

QUESTION NO: 920

Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?

A. Degaussing
B. Defragmenting
C. Erasing
D. Destroying

Answer: D
Explanation:
Destroying magnetic media is the only way to assure that confidential information cannot be recovered. Degaussing or demagnetizing is not sufficient to fully erase information from magnetic mediA. The purpose of defragmentation is to eliminate fragmentation in file systems and does not remove information. Erasing or deleting magnetic media does not remove the information; this method simply changes a file's indexing information.

QUESTION NO: 921

Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

A. Policies that require instant dismissal if such devices are found
B. Software for tracking and managing USB storage devices
C. Administratively disabling the USB port
D. Searching personnel for USB storage devices at the facility's entrance

Answer: B
Explanation:
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissalmay result in increased employee attrition and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching of personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

QUESTION NO: 922

An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

A. Run a low-level data wipe utility on all hard drives
B. Erase all data file directories
C. Format all hard drives
D. Physical destruction of the hard drive

Answer: D
Explanation:
The most effective method is physical destruction. Running a low-level data wipe utility may leave some residual data that could be recovered; erasing data directories and formatting hard drives are easily reversed, exposing all data on the drive to unauthorized individuals.

QUESTION NO: 923

To ensure authentication, confidentiality and integrity of a message, the sender should

encrypt the hash of the message with the sender's:

A. public key and then encrypt the message with the receiver's private key.
B. private key and then encrypt the message with the receiver's public key.
C. public key and then encrypt the message with the receiver's public key.
D. private key and then encrypt the message with the receiver's private key.

Answer: B
Explanation:

Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

QUESTION NO: 924

Which of the following would be the MOST significant audit finding when reviewing a

point-of-sale (POS) system?

A. invoices recorded on the POS system are manually entered into an accounting application
B. An optical scanner is not used to read bar codes for the generation of sales invoices
C. Frequent power outages occur, resulting in the manual preparation of invoices
D. Customer credit card information is stored unencrypted on the local POS system

Answer: D
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 NO: 925

When reviewing the procedures for the disposal of computers, which of the following

should be the GREATEST concern for the IS auditor?

A. Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
B. All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
C. Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
D. 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.

Answer: B
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 fromshredded hard disks is virtually impossible, especially when the scrap is mixed with other metal parts. If the transport can be secured and the destruction be proved as described in the option, this is a valid method of disposal.

QUESTION NO: 926

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?

A. The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
B. The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
C. Timely synchronization is ensured by policies and procedures.
D. The usage of the handheld computers is allowed by the hospital policy.

Answer: A
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.

Topic 7, BUSINESS CONTINUITY AND DISASTER RECOVERY (111 PRACTICE QUESTIONS)

QUESTION NO: 927

Which of the following would BEST support 24/7 availability?

A. Daily backup
B. Offsite storage

C. Mirroring
D. Periodic testing

Answer: C
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 NO: 928

The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

A. achieve performance improvement.
B. provide user authentication.
C. ensure availability of data.
D. ensure the confidentiality of data.

Answer: C
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 NO: 929

Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

A. physically separated from the data center and not subject to the same risks.
B. given the same level of protection as that of the computer data center.
C. outsourced to a reliable third party.
D. equipped with surveillance capabilities.

Answer: A
Explanation:
It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location

selection.

QUESTION NO: 930

If a database is restored using before-image dumps, where should the process begin following an interruption?

A. Before the last transaction
B. After the last transaction
C. As the first transaction after the latest checkpoint
D. As the last transaction before the latest checkpoint

Answer: A
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 NO: 931

In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

A. Maintaining system software parameters
B. Ensuring periodic dumps of transaction logs
C. Ensuring grandfather-father-son file backups
D. Maintaining important data at an offsite location

Answer: B
Explanation:
Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical datA. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

QUESTION NO: 932

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?

A. The previous day's backup file and the current transaction tape
B. The previous day's transaction file and the current transaction tape

C. The current transaction tape and the current hard copy transaction log
D. The current hard copy transaction log and the previous day's transaction file

Answer: A
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 upto the point of interruption.

QUESTION NO: 933

An offsite information processing facility:

A. should have the same amount of physical access restrictions as the primary processing site.
B. should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
C. should be located in proximity to the originating site, so it can quickly be made operational.
D. need not have the same level of environmental monitoring as the originating site.

Answer: A
Explanation:
An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity of the original site. The offsite facility should possess the same level of environmental monitoring and control as the originating site.

QUESTION NO: 934

An IS auditor performing a review of the backup processing facilities should be MOST concerned that:

A. adequate fire insurance exists.
B. regular hardware maintenance is performed.
C. offsite storage of transaction and master files exists.
D. backup processing facilities are fully tested.

Answer: C
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 NO: 935

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

A. Reviewing program code
B. Reviewing operations documentation
C. Turning off the UPS, then the power
D. Reviewing program documentation

Answer: B
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 NO: 936

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?

A. There are three individuals with a key to enter the area.
B. Paper documents are also stored in the offsite vault.
C. Data files that are stored in the vault are synchronized.
D. The offsite vault is located in a separate facility.

Answer: C
Explanation:
Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

QUESTION NO: 937

Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

A. database integrity checks.
B. validation checks.

C. input controls.
D. database commits and rollbacks.

Answer: D
Explanation:
Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

QUESTION NO: 938

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

A. located on a different floor of the building.
B. easily accessible by everyone.
C. clearly labeled for emergency access.
D. protected from unauthorized access.

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

QUESTION NO: 939

Which of the following ensures the availability of transactions in the event of a disaster?

A. Send tapes hourly containing transactions offsite,
B. Send tapes daily containing transactions offsite.
C. Capture transactions to multiple storage devices.
D. Transmit transactions offsite in real time.

Answer: D
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 availabilityat an offsite location.

QUESTION NO: 940

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:

A. upgrading to a level 5 RAID.
B. increasing the frequency of onsite backups.
C. reinstating the offsite backups.
D. establishing a cold site in a secure location.

Answer: C
Explanation:
A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups, more frequent onsite backups or even setting up a cold site. Choices A, B and D do not compensate for the lack of offsite backup.

QUESTION NO: 941

In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?

A. Disaster tolerance is high.
B. Recovery time objective is high.
C. Recovery point objective is low.
D. Recovery point objective is high.

Answer: C
Explanation:
A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the datA. If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of the disaster tolerance. The lower the RTO, the lower the disaster tolerance. Therefore, choice C is the correct answer.

QUESTION NO: 942

Network Data Management Protocol (NDMP) technology should be used for backup if:

A. a network attached storage (NAS) appliance is required.
B. the use of TCP/I P must be avoided.
C. file permissions that can not be handled by legacy backup systems must be backed up.
D. backup consistency over several related data volumes must be ensured.

Answer: A

Explanation:

NDMP defines three kind of services: a data service that interfaces with the primary storage to be backed up or restored, a tape service that interfaces with the secondary storage (primarily a tape device), and a translator service performing translations including multiplexing multiple data streams into one data stream and vice versA. NDMP services interact with each other. The result of this interaction is the establishment of an NDMP control session if the session is being used to achieve control for the backup or restore operation. It would result in an NDMP data session if the session is being used to transfer actual file system or volume data (including metadata). Control sessions are always TCP/IP-based, but data streams can be TCP/lP-or SAN-based. NDMP is more or less NAS-centric and defines a way to back up and restore data from a device, such as a NAS appliance, on which it is difficult to install a backup software agent, in the absence of NDMP, this data must be backed up as a shared drive on the LAN, which is accessed via network file protocols, such as Common Internet File System (CIFS) or Network File System (NFS), degrading backup performance. NDMP works on a block level for transferring payload data (file content)but metadata and traditional file system information needs to be handled by legacy backup systems that initiate NDMP data movement. NDMP does not know about nor takes care of consistency issues regarding related volumes (e.g., a volume to store data

QUESTION NO: 943

An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to-disk solution. This is appropriate because:

A. fast synthetic backups for offsite storage are supported.
B. backup to disk is always significantly faster than backup to tape.
C. tape libraries are no longer needed.
D. data storage on disks is more reliable than on tapes.

Answer: A

Explanation:

Disk-to-disk (D2D) backup should not be seen as a direct replacement for backup to tape; rather, it should be viewed as part of a multitiered backup architecture that takes advantage of the best features of both tape and disk technologies. Backups todisks are not dramatically faster than backups to tapes in a balanced environment. Most often than not there is hardly a difference, since the limiting components are not tape or disk drives but the overall sustained bandwidth of the backup server'sbackplane. The advantage in terms of speed is in restoring performance, since all data are on hand and can be accessed randomly, resulting in a dramatic enhancement in throughput. This makes fast synthetic backups (making a full backup without touching the host's data only by using the existing incremental backups) efficient and easy. Although the cost of disks has been reduced, tape-based backup can offer an overall cost advantage over disk-only solutions. Even if RAID arrays are used for D2Dstorage, a failed drive must be swapped out and the RAID set rebuilt before another disk drive fails, thus making this kind of backup more risky and not suitable as a solution of last resort. In contrast, a single tape drive failure does not produceany data loss since the data resides on the tape mediA. In a multidrive library, the loss of the use of a single tape drive has no impact on the overall level of data protection. Conversely, the loss of a disk drive in an array can put all data at ri

QUESTION NO: 944

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?

A. Full backup window
B. Media costs
C. Restore window
D. Media reliability

Answer: D
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 NO: 945

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?

A. Daily data backup to tape and storage at a remote site
B. Real-time replication to a remote site
C. Hard disk mirroring to a local server
D. Real-time data backup to the local storage area network (SAN)

Answer: B
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 NO: 946

Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?

A. Virtual tape libraries
B. Disk-based snapshots
C. Continuous data backup
D. Disk-to-tape backup

Answer: C
Explanation:
The recovery point objective (RPO) is based on the acceptable data loss in the case of a disruption. In this scenario the organization needs a short RPO. Virtual tape libraries, disk-based snapshots and disk-to-tape backup would require time to complete the backup, while continuous data backup happens online (in real time).

QUESTION NO: 947

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

A. Weekly full backup with daily incremental backup
B. Daily full backup
C. Clustered servers
D. Mirrored hard disks

Answer: A
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 beimpractical to conduct a full backup 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 NO: 948

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:

A. the level of information security required when business recovery procedures are invoked.
B. information security roles and responsibilities in the crisis management structure.
C. information security resource requirements.
D. change management procedures for information security that could affect business continuity

arrangements.

Answer: A

Explanation:

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

QUESTION NO: 949

Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

A. Backup time would steadily increase
B. Backup operational cost would significantly increase
C. Storage operational cost would significantly increase
D. Server recovery work may not meet the recovery time objective (RTO)

Answer: D

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 ensurethat 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 NO: 950

Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

A. Minimum operating requirements
B. Acceptable data loss
C. Mean time between failures
D. Acceptable time for recovery

Answer: B

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 NO: 951

A structured walk-through test of a disaster recovery plan involves:

A. representatives from each of the functional areas coming together to go over the plan.
B. all employees who participate in the day-to-day operations coming together to practice executing the plan.
C. moving the systems to the alternate processing site and performing processing operations.
D. distributing copies of the plan to the various functional areas for review.

Answer: B
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 NO: 952

In a contract with a hot, warm or cold site, contractual provisions should cover which of the following considerations?

A. Physical security measures
B. Total number of subscribers
C. Number of subscribers permitted to use a site at one time
D. References by other users

Answer: C
Explanation:
The contract should specify the number of subscribers permitted to use the site at any one time. Physical security measures are not a part of the contract, although they are an important consideration when choosing a third-party site. The total number of subscribers is not a consideration; what is important is whether the agreement limits the number of subscribers in a building or in a specific areA. The references that other users can provide is a consideration taken before signing the contract; it is by no means part of the contractual provisions.

QUESTION NO: 953
Which of the following is the GREATEST concern when an organization's backup facility is at a

warm site?

A. Timely availability of hardware
B. Availability of heat, humidity and air conditioning equipment
C. Adequacy of electrical power connections
D. Effectiveness of the telecommunications network

Answer: A
Explanation:
A warm site has the basic infrastructure facilities implemented, such as power, air conditioning and networking, but is normally lacking computing equipment. Therefore, the availability of hardware becomes a primary concern.

QUESTION NO: 954

Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

A. A hot site maintained by the business
B. A commercial cold site
C. A reciprocal arrangement between its offices
D. A third-party hot site

Answer: C
Explanation:
For a business having many offices within a region, a reciprocal arrangement among its offices would be most appropriate. Each office could be designated as a recovery site for some other office. This would be the least expensive approach to providing an acceptable level of confidence. A hot site maintained by the business would be a costly solution but would provide a high degree of confidence. Multiple cold sites leased for the multiple offices would lead to a costly solution with a high degree of confidence. A third-party facility for recovery is provided by a traditional hot site. This would be a costly approach providing a high degree of confidence.

QUESTION NO: 955

The PRIMARY purpose of a business impact analysis (BIA) is to:

A. provide a plan for resuming operations after a disaster.
B. identify the events that could impact the continuity of an organization's operations.
C. publicize the commitment of the organization to physical and logical security.
D. provide the framework for an effective disaster recovery plan.

Answer: B
Explanation:

A business impact analysis (BIA) is one of the key steps in the development of a business continuity plan (BCP). A BIA will identify the diverse events that could impact the continuity of the operations of an organization.

QUESTION NO: 956

After implementation of a disaster recovery plan, pre-disaster and post-disaster operational costs for an organization will:

A. decrease.
B. not change (remain the same).
C. increase.
D. increase or decrease depending upon the nature of the business.

Answer: C
Explanation:
There are costs associated with all activities and disaster recovery planning (DRP) is not an exception. Although there are costs associated with a disaster recovery plan, there are unknown costs that are incurred if a disaster recovery plan is not implemented.

QUESTION NO: 957

Which of the following is the MOST reasonable option for recovering a noncritical system?

A. Warm site
B. Mobile site
C. Hot site
D. Cold site

Answer: D
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 uponthe 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 NO: 958

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan. Using actual resources, which of the following is the MOST cost-effective test of the disaster recovery plan?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

Answer: B
Explanation:
A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for 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 NO: 959

An organization's disaster recovery plan should address early recovery of:

A. all information systems processes.
B. all financial processing applications.
C. only those applications designated by the IS manager.
D. processing in priority order, as defined by business management.

Answer: D
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 NO: 960

An advantage of the use of hot sites as a backup alternative is that:

A. the costs associated with hot sites are low.
B. hot sites can be used for an extended amount of time.
C. hot sites can be made ready for operation within a short period of time.
D. they do not require that equipment and systems software be compatible with the primary site.

Answer: C
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 NO: 961

Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

A. Invite client participation.
B. involve all technical staff.
C. Rotate recovery managers.
D. install locally-stored backup.

Answer: C
Explanation:
Recovery managers should be rotated to ensure the experience of the recovery plan is spread among the managers. Clients may be involved but not necessarily in every case. Not all technical staff should be involved in each test. Remote or offsite backup should always be used.

QUESTION NO: 962

Disaster recovery planning (DRP) addresses the:

A. technological aspect of business continuity planning.
B. operational piece of business continuity planning.
C. functional aspect of business continuity planning.
D. overall coordination of business continuity planning.

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

QUESTION NO: 963

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial

processing organization has discovered the following:

- The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.

- The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.

- The plan has never been updated, tested or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The IS auditor's report should recommend that:

A. the deputy CEO be censured for their failure to approve the plan.
B. a board of senior managers is set up to review the existing plan.
C. the existing plan is approved and circulated to all key management and staff.
D. a manager coordinates the creation of a new or revised plan within a defined time limit.

Answer: D
Explanation:
The primary concern is to establish a workable disaster recovery plan, which reflects current processing volumes to protect the organization from any disruptive incident. Censuring the deputy CEO will not achieve this and is generally not within the scope of an IS auditor to recommend. Establishing a board to review the plan, which is two years out of date, may achieve an updated plan, but is not likely to be a speedy operation, and issuing the existing plan would be folly without first ensuring that it is workable. The best way to achieve a disaster recovery plan in a short time is to make an experienced manager responsible for coordinating the knowledge of other managers into a single, formal document within a defined time limit.

QUESTION NO: 964

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:

A. take no action as the lack of a current plan is the only significant finding.
B. recommend that the hardware configuration at each site is identical.

C. perform a review to verify that the second configuration can support live processing.
D. report that the financial expenditure on the alternative site is wasted without an effective plan.

Answer: C
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.

QUESTION NO: 965

Disaster recovery planning (DRP) for a company's computer system usually focuses on:

A. operations turnover procedures.
B. strategic long-range planning.
C. the probability that a disaster will occur.
D. alternative procedures to process transactions.

Answer: D
Explanation:
It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

QUESTION NO: 966

The MAIN purpose for periodically testing offsite facilities is to:

A. protect the integrity of the data in the database.
B. eliminate the need to develop detailed contingency plans.
C. ensure the continued compatibility of the contingency facilities.
D. ensure that program and system documentation remains current.

Answer: C
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 NO: 967

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?

A. Offsite storage of daily backups
B. Alternative standby processor onsite
C. installation of duplex communication links
D. Alternative standby processor at another network node

Answer: D
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 allof 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 ofan 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 NO: 968

Facilitating telecommunications continuity by providing redundant combinations of local carrier T-1 lines, microwaves and/or coaxial cables to access the local communication loop:

A. last-mile circuit protection.
B. long-haul network diversity.
C. diverse routing.
D. alternative routing.

Answer: A
Explanation:
The method of providing telecommunication continuity through the use of many recovery facilities, providing redundant combinations of local carrier T-ls, microwave and/or coaxial cable to access the local communication loop in the event of a disaster, is called last-mile circuit protection. Providing diverse long-distance network availability utilizing T-l circuits among major long-distance carriers is called long-haul network diversity. This ensures long-distance access should any one

carrier experience a network failure. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

QUESTION NO: 969

Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

A. Developments may result in hardware and software incompatibility.
B. Resources may not be available when needed.
C. The recovery plan cannot be tested.
D. The security infrastructures in each company may be different.

Answer: A
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.

QUESTION NO: 970

Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

A. Built-in alternative routing
B. Completing full system backup daily
C. A repair contract with a service provider
D. A duplicate machine alongside each server

Answer: A
Explanation:
Alternative routing would ensure the network would continue if a server is lost or if a link is severed as message rerouting could be automatic. System backup will not afford immediate protection. The repair contract is not as effective as perm a nentalte (native routing. Standby servers will not provide continuity if a link is severed.

QUESTION NO: 971

An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

A. tested every six months.
B. regularly reviewed and updated.
C. approved by the chief executive officer (CEO).
D. communicated to every department head in the organization.

Answer: B
Explanation:
The plan should be reviewed at appropriate intervals, depending upon the nature of the business and the rate of change of systems and personnel. Otherwise, it may become out of date and may no longer be effective. The plan must be subjected to regular testing, but the period between tests will again depend on the nature of the organization and the relative importance of IS. Three months or even annually may be appropriate in different circumstances. Although the disaster recovery plan should receive the approval of senior management, it need not be the CEO if another executive officer is equally or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan. Similarly, although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communications staff.

QUESTION NO: 972

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

A. alternative routing.
B. diverse routing.
C. long-haul network diversity.
D. last-mile circuit protection.

Answer: B
Explanation:
Diverse routing routes traffic through split-cable facilities or duplicate-cable facilities. This can be accomplished with different and/or duplicate cable sheaths, if different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual-entrance facilities. This type of access is time consuming and costly. Alternative routing is a method of routing information via an alternate medium, such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be

unavailable. Long-haul network diversity is a diverse, long-distance network utilizing T-l circuits among the major long-distance carriers. It ensures long-distance access should any carrier experience a network failure. Last-mile circuit protection is a redundant combination of local carrier T-ls, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local-carrier routing is also utilized.

QUESTION NO: 973

The responsibilities of a disaster recovery relocation team include:

A. obtaining, packaging and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
B. locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
C. managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
D. coordinating the process of moving from the hot site to a new location or to the restored original location.

Answer: D
Explanation:
Choice A describes an offsite storage team, choice B defines a transportation team and choice C defines a salvage team.

QUESTION NO: 974

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?

A. Deterrence
B. Mitigation
C. Recovery
D. Response

Answer: B
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 NO: 975

Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

A. The alternate facility will be available until the original information processing facility is restored.
B. User management is involved in the identification of critical systems and their associated critical recovery times.
C. Copies of the plan are kept at the homes of key decision-making personnel.
D. Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Answer: A
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 of the plan.

QUESTION NO: 976

Which of the following must exist to ensure the viability of a duplicate information processing facility?

A. The site is near the primary site to ensure quick and efficient recovery.
B. The site contains the most advanced hardware available.
C. The workload of the primary site is monitored to ensure adequate backup is available.
D. The hardware is tested when it is installed to ensure it is working properly.

Answer: C
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.

QUESTION NO: 977

An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

A. cold site.

B. warm site.
C. dial-up site.
D. duplicate processing facility.

Answer: A
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 NO: 978

A disaster recovery plan for an organization should:

A. reduce the length of the recovery time and the cost of recovery.
B. increase the length of the recovery time and the cost of recovery.
C. reduce the duration of the recovery time and increase the cost of recovery.
D. affect neither the recovery time nor the cost of recovery.

Answer: A
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 NO: 979

A disaster recovery plan for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

A. A hot site that can be operational in eight hours with asynchronous backup of the transaction logs
B. Distributed database systems in multiple locations updated asynchronously
C. Synchronous updates of the data and standby active systems in a hot site
D. Synchronous remote copy of the data in a warm site that can be operational in 48 hours

Answer: D
Explanation:
The synchronous copy of the storage achieves the RPO objective and a warm site operational in

48 hours meets the required RTO. Asynchronous updates of the database in distributed locations do not meet the RPO. Synchronous updates of the data and standby active systems in a hot site meet the RPO and RTO requirements but are more costly than a warm site solution.

QUESTION NO: 980

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?

A. Reciprocal agreement with another organization
B. Alternate processor in the same location
C. Alternate processor at another network node
D. Installation of duplex communication links

Answer: C
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 NO: 981

The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will MOST likely:

A. increase.
B. decrease.
C. remain the same.
D. be unpredictable.

Answer: A
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 morethan the cost of operations during a nondisaster period when no disaster recovery plan was in place.

QUESTION NO: 982

Which of the following tasks should be performed FIRST when preparing a disaster recovery plan?

A. Develop a recovery strategy.
B. Perform a business impact analysis.
C. Map software systems, hardware and network components.
D. Appoint recovery teams with defined personnel, roles and hierarchy.

Answer: B
Explanation:
The first step in any disaster recovery plan is to perform a business impact analysis. All other tasks come afterwards.

QUESTION NO: 983

Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

A. A disaster recovery plan
B. Customer references for the alternate site provider
C. Processes for maintaining the disaster recovery plan
D. Results of tests and drills

Answer: D
Explanation:
Plans are important, but mere plans do not provide reasonable assurance unless tested. References for the alternate site provider and the existence and maintenance of a disaster recovery plan are important, but only tests and drills demonstrate the adequacy of the plans and provide reasonable assurance of an organization's disaster recovery readiness.

QUESTION NO: 984

Which of the following is the BEST method for determining the criticality of each application system in the production environment?

A. interview the application programmers.
B. Perform a gap analysis.
C. Review the most recent application audits.
D. Perform a business impact analysis.

Answer: D
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 NO: 985

A hot site should be implemented as a recovery strategy when the:

A. disaster tolerance is low.
B. recovery point objective (RPO) is high.
C. recovery time objective (RTO) is high.
D. disaster tolerance is high.

Answer: A
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 NO: 986

An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

A. Obtain senior management sponsorship.
B. Identify business needs.
C. Conduct a paper test.
D. Perform a system restore test.

Answer: C
Explanation:
A best practice would be to conduct a paper test. Senior management sponsorship and business needs identification should have been obtained prior to implementing the plan. A paper test should be conducted first, followed by system or full testing.

QUESTION NO: 987

When auditing a disaster recovery plan for a critical business area, an IS auditor finds that it does not cover all the systems. Which of the following is the MOST appropriate action for the IS auditor?

A. Alert management and evaluate the impact of not covering all systems.
B. Cancel the audit.
C. Complete the audit of the systems covered by the existing disaster recovery plan.
D. Postpone the audit until the systems are added to the disaster recovery plan.

Answer: A
Explanation:
An IS auditor should make management aware that some systems are omitted from the disaster recovery plan. An IS auditor should continue the audit and include an evaluation of the impact of not including all systems in the disaster recovery plan. Cancelling the audit, ignoring the fact that some systems are not covered or postponing the audit are inappropriate actions to take.

QUESTION NO: 988

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

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

Answer: D
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 NO: 989

Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

A. all threats can be completely removed.
B. a cost-effective, built-in resilience can be implemented.
C. the recovery time objective can be optimized.
D. the cost of recovery can be minimized.

Answer: B

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 NO: 990

An organization has a number of branches across a wide geographical areA. To ensure that all aspects of the disaster recovery plan are evaluated in a cost effective manner, an IS auditor should recommend the use of a:

A. data recovery test.
B. full operational test.
C. posttest.
D. preparedness test.

Answer: D

Explanation:

A preparedness test should be performed by each local office/area to test the adequacy of the preparedness of local operations in the event of a disaster. This test should be performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence of the plan's adequacy. A data recovery test is a partial test and will not ensure that all aspects are evaluated. A full operational test is not the most cost effective test in light of the geographical dispersion of the branches, and a posttest is a phase of the test execution process.

QUESTION NO: 991

If the recovery time objective (RTO) increases:

A. the disaster tolerance increases.
B. the cost of recovery increases.
C. a cold site cannot be used.
D. the data backup frequency increases.

Answer: A

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 NO: 992

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?

A. Catastrophic service interruption
B. High consumption of resources
C. Total cost of the recovery may not be minimized
D. Users and recovery teams may face severe difficulties when activating the plan

Answer: A

Explanation:

Choices B, C and D are all possible problems that might occur, and would cause difficulties and financial losses or waste of resources. However, if a new disaster recovery plan is not tested, the possibility of a catastrophic service interruption is the most critical of all risks.

QUESTION NO: 993

When developing a disaster recovery plan, the criteria for determining the acceptable downtime should be the:

A. annualized loss expectancy (ALE).
B. service delivery objective.
C. quantity of orphan data.
D. maximum tolerable outage.

Answer: D

Explanation:

The recovery time objective is determined based on the acceptable downtime in case of a disruption of operations, it indicates the maximum tolerable outage that an organization considers to be acceptable before a system or process must resume following a disaster. Choice A is incorrect, because the acceptable downtime would not be determined by the annualized loss expectancy (ALE). Choices B and C are relevant to business continuity, but they are not determined by acceptable downtime.

QUESTION NO: 994

A lower recovery time objective (RTO) results in:

A. higher disaster tolerance.
B. higher cost.
C. wider interruption windows.
D. more permissive data loss.

Answer: B

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 thelesserthe permissive data loss.

QUESTION NO: 995

Regarding a disaster recovery plan, the role of an IS auditor should include:

A. identifying critical applications.
B. determining the external service providers involved in a recovery test.
C. observing the tests of the disaster recovery plan.
D. determining the criteria for establishing a recovery time objective (RTO).

Answer: C

Explanation:

The IS auditor should be present when disaster recovery plans are tested, to ensure that the test meets the targets for restoration, and the recovery procedures are effective and efficient. As appropriate, the auditor should provide a report of the test results. All other choices are a responsibility of management.

QUESTION NO: 996

During a disaster recovery test, an IS auditor observes that the performance of the

disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:

A. event error log generated at the disaster recovery site.
B. disaster recovery test plan.
C. disaster recovery plan (DRP).
D. configurations and alignment of the primary and disaster recovery sites.

Answer: D

Explanation:

Since the configuration of the system is the most probable cause, the IS auditor should review that first. If the issue cannot be clarified, the IS auditor should then review the event error log. The disaster recovery test plan and the disaster recovery plan (DRP) would not contain information about the system configuration.

QUESTION NO: 997

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. a data loss of up to 1 minute, but the processing must be continuous.
B. a 1-minute processing interruption but cannot tolerate any data loss.
C. a processing interruption of 1 minute or more.
D. both a data loss and a processing interruption longer than 1 minute.

Answer: A
Explanation:
The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery point objective (RPO) measures how much data loss can be accepted. Choices B, C and D are incorrect since they exceed the RTO limits set by the scenario.

QUESTION NO: 998

Which of the following issues should be the GREATEST concern to the IS auditor when

reviewing an IT disaster recovery test?

A. 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.
B. 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.
C. The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
D. Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Answer: D
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 arenot 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 theyear. 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 NO: 999

The frequent updating of which of the following is key to the continued effectiveness of a

disaster recovery plan (DRP)?

A. Contact information of key personnel
B. Server inventory documentation
C. individual roles and responsibilities
D. Procedures for declaring a disaster

Answer: A
Explanation:
In the event of a disaster, it is important to have a current updated list of personnel who are key to the operation of the plan. Choices B, C and D would be more likely to remain stable overtime.

QUESTION NO: 1000

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:

A. system and the IT operations team can sustain operations in the emergency environment.
B. resources and the environment could sustain the transaction load.
C. connectivity to the applications at the remote site meets response time requirements.
D. workflow of actual business operations can use the emergency system in case of a disaster.

Answer: A
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 NO: 1001

To address an organization's disaster recovery requirements, backup intervals should not exceed the:

A. service level objective (SLO).
B. recovery time objective (RTO).
C. recovery point objective (RPO).
D. maximum acceptable outage (MAO).

Answer: C

Explanation:

The recovery point objective (RPO) defines the point in time to which data must be restored after a disaster so as to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If service levels are not met, the usual consequences are penalty payments, not cessation of business. Organizations will try to set service level objectives (SLOs) so as to meet established targets. The resulting time for the service level agreement (SLA) will usually be longer than the RPO. The recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored. The maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for RTO. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

QUESTION NO: 1002

Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?

A. Resuming critical processes
B. Recovering sensitive processes
C. Restoring the site
D. Relocating operations to an alternative site

Answer: A

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 NO: 1003

After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

A. Test and maintain the plan.
B. Develop a specific plan.
C. Develop recovery strategies.
D. implement the plan.

Answer: C

Explanation:

The next phase in the continuity plan development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster. After selecting a strategy, a specific plan can be developed, tested and implemented.

QUESTION NO: 1004

Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

A. Pilot
B. Paper
C. Unit
D. System

Answer: B

Explanation:

A paper test is appropriate for testing a BCP. it is a walkthrough of the entire plan, or part of the plan, involving major players in the plan's execution, who reason out what may happen in a particular disaster. Choices A, C and D are not appropriate for a BCP.

QUESTION NO: 1005

An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

A. Nonavailability of an alternate private branch exchange (PBX) system
B. Absence of a backup for the network backbone
C. Lack of backup systems for the users' PCs
D. Failure of the access card system

Answer: B

Explanation:

Failure of a network backbone will result in the failure of the complete network and impact the ability of all users to access information on the network. The nonavailability of an alternate PBX system will result in users not being able to make or receive telephone calls or faxes; however, users may have alternate means of communication, such as a mobile phone or e-mail. Lack of backup systems for user PCs will impact only the specific users, not all users. Failure of the access card system impacts the ability to maintain records of the users who are entering the specified work areas; however, this could be mitigated by manual monitoring controls.

QUESTION NO: 1006

As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

A. Organizational risks, such as single point-of-failure and infrastructure risk
B. Threats to critical business processes
C. Critical business processes for ascertaining the priority for recovery
D. Resources required for resumption of business

Answer: C
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 NO: 1007

Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

A. Verify compatibility with the hot site.
B. Review the implementation report.
C. Perform a walk-through of the disaster recovery plan.
D. Update the IS assets inventory.

Answer: D
Explanation:
An IS assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IS infrastructure. The other choices are procedures required to update the disaster recovery plan after having updated the required assets inventory.

QUESTION NO: 1008

Which of the following would contribute MOST to an effective business continuity plan (BCP)?

A. Document is circulated to all interested parties
B. Planning involves all user departments
C. Approval by senior management
D. Audit by an external IS auditor

Answer: B
Explanation:

The involvement of user departments in the BCP is crucial for the identification of the business processing priorities. The BCP circulation will ensure that the BCP document is received by all users. Though essential, this does not contribute significantly to the success of the BCP. A BCP approved by senior management would not ensure the quality of the BCP, nor would an audit necessarily improve the quality of the BCP.

QUESTION NO: 1009

To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

A. Business recovery strategy
B. Detailed plan development
C. Business impact analysis (BIA)
D. Testing and maintenance

Answer: C
Explanation:
End user involvement is critical in the BIA phase. During this phase the current operations of the business needs to be understood and the impact on the business of various disasters must be evaluated. End users are the appropriate persons to provide relevant information for these tasks, inadequate end user involvement in this stage could result in an inadequate understanding of business priorities and the plan not meeting the requirements of the organization.

QUESTION NO: 1010

Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

A. A hot site is contracted for and available as needed.
B. A business continuity manual is available and current.
C. insurance coverage is adequate and premiums are current.
D. Media backups are performed on a timely basis and stored offsite.

Answer: D
Explanation:
Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

QUESTION NO: 1011

The PRIMARY objective of business continuity and disaster recovery plans should be to:

A. safeguard critical IS assets.
B. provide for continuity of operations.
C. minimize the loss to an organization.
D. protect human life.

Answer: D

Explanation:

Since human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people. All other priorities are important but are secondary objectives of a business continuity and disaster recovery plan.

QUESTION NO: 1012

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?

A. Perform an integral review of the recovery tasks.
B. Broaden the processing capacity to gain recovery time.
C. Make improvements in the facility's circulation structure.
D. increase the amount of human resources involved in the recovery.

Answer: A

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.

QUESTION NO: 1013

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?

A. Paper test
B. Post test
C. Preparedness test
D. Walkthrough

Answer: C

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments. A paper test is a walkthrough of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution. A paper test usually precedes the preparedness test. A post-test is actually a test phase and is comprised of a group of activities, such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third-party systems. A walkthrough is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff, rather than the actual resources.

QUESTION NO: 1014

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:

A. shadow file processing.
B. electronic vaulting.
C. hard-disk mirroring.
D. hot-site provisioning.

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

QUESTION NO: 1015

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:

A. each plan is consistent with one another.
B. all plans are integrated into a single plan.
C. each plan is dependent on one another.
D. the sequence for implementation of all plans is defined.

Answer: A

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 tobe 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 NO: 1016

During a business continuity audit an IS auditor found that the business continuity plan

(BCP) covered only critical processes. The IS auditor should:

A. recommend that the BCP cover all business processes.
B. assess the impact of the processes not covered.
C. report the findings to the IT manager.
D. redefine critical processes.

Answer: B

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 NO: 1017

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?

A. Recommend that an additional comprehensive BCP be developed.
B. Determine whether the BCPs are consistent.
C. Accept the BCPs as written.
D. Recommend the creation of a single BCP.

Answer: B

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 NO: 1018

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?

A. Business continuity self-audit
B. Resource recovery analysis
C. Risk assessment
D. Gap analysis

Answer: C
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 NO: 1019

During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

A. Evacuation plan
B. Recovery priorities
C. Backup storages
D. Call tree

Answer: A
Explanation:
Protecting human resources during a disaster-related event should be addressed first. Having separate BCPs could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients. Choices B, C and D may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.

QUESTION NO: 1020

Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

A. downtime costs.
B. resumption costs.
C. recovery costs.
D. walkthrough costs.

Answer: A

Explanation:

Since the recovery time is longer in plan B, resumption and recovery costs can be expected to be lower. Walkthrough costs are not a part of disaster recovery. Since the management considered a higher window for recovery in plan B, downtime costs included in the plan are likely to be higher.

QUESTION NO: 1021

The optimum business continuity strategy for an entity is determined by the:

A. lowest downtime cost and highest recovery cost.
B. lowest sum of downtime cost and recovery cost.
C. lowest recovery cost and highest downtime cost.
D. average of the combined downtime and recovery cost.

Answer: B

Explanation:

Both costs have to be minimized, and the strategy for which the costs are lowest is the optimum strategy. The strategy with the highest recovery cost cannot be the optimum strategy. The strategy with the highest downtime cost cannot be the optimum strategy. The average of the combined downtime and recovery cost will be higher than the lowest combined cost of downtime and recovery.

QUESTION NO: 1022

The PRIMARY objective of testing a business continuity plan is to:

A. familiarize employees with the business continuity plan.
B. ensure that all residual risks are addressed.
C. exercise all possible disaster scenarios.
D. identify limitations of the business continuity plan.

Answer: D

Explanation:

Testing the business continuity plan provides the best evidence of any limitations that may exist. Familiarizing employees with the business continuity plan is a secondary benefit of a test. It is not cost effective to address residual risks in a business continuity plan, and it is not practical to test all possible disaster scenarios.

QUESTION NO: 1023

In determining the acceptable time period for the resumption of critical business processes:

A. only downtime costs need to be considered.
B. recovery operations should be analyzed.
C. both downtime costs and recovery costs need to be evaluated.
D. indirect downtime costs should be ignored.

Answer: C
Explanation:
Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis (BIA) should be a recovery strategy that represents the optimal balance. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to recover information resources might be prohibitive for nonessential business processes. Recovery operations do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows incurred due to business disruption. The indirect costs of a serious disruption to normal business activity, e.g., loss of customer and supplier goodwill and loss of market share, may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

QUESTION NO: 1024

In the event of a disruption or disaster, which of the following technologies provides for continuous operations?

A. Load balancing
B. Fault-tolerant hardware
C. Distributed backups
D. High-availability computing

Answer: B
Explanation:
Fault-tolerant hardware is the only technology that currently supports continuous, uninterrupted

service. Load balancing is used to improve the performance of the server by splitting the work between several servers based on workloads. High-availability (HA) computing facilities provide a quick but not continuous recovery, while distributed backups require longer recovery times.

QUESTION NO: 1025

Which of the following would be MOST important for an IS auditor to verify when conducting a business continuity audit?

A. Data backups are performed on a timely basis
B. A recovery site is contracted for and available as needed
C. Human safety procedures are in place
D. insurance coverage is adequate and premiums are current

Answer: C
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 NO: 1026

Which of the following insurance types provide for a loss arising from fraudulent acts by employees?

A. Business interruption
B. Fidelity coverage
C. Errors and omissions
D. Extra expense

Answer: B
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 NO: 1027

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

A. plans and compare them to appropriate standards.
B. results from previous tests.
C. emergency procedures and employee training.
D. offsite storage and environmental controls.

Answer: B
Explanation:
Previous test results will provide evidence of the effectiveness of the business continuity plan. Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness. Reviewing emergency procedures, offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

QUESTION NO: 1028

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:

A. clarity and simplicity of the business continuity plans.
B. adequacy of the business continuity plans.
C. effectiveness of the business continuity plans.
D. ability of IS and end-user personnel to respond effectively in emergencies.

Answer: A
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 NO: 1029

During the design of a business continuity plan, the business impact analysis (BIA) identifies critical processes and supporting applications. This will PRIMARILY influence the:

A. responsibility for maintaining the business continuity plan.
B. criteria for selecting a recovery site provider.
C. recovery strategy.
D. responsibilities of key personnel.

Answer: C
Explanation:
The most appropriate strategy is selected based on the relative risk level and criticality identified in the business impact analysis (BIA.) The other choices are made after the selection or design of the appropriate recovery strategy.

QUESTION NO: 1030

During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The MAJOR risk associated with this is that:

A. assessment of the situation may be delayed.
B. execution of the disaster recovery plan could be impacted.
C. notification of the teams might not occur.
D. potential crisis recognition might be ineffective.

Answer: B
Explanation:
Execution of the business continuity plan would be impacted if the organization does not know when to declare a crisis. Choices A, C and D are steps that must be performed to know whether to declare a crisis. Problem and severity assessment would provide information necessary in declaring a disaster. Once a potential crisis is recognized, the teams responsible for crisis management need to be notified. Delaying this step until a disaster has been declared would negate the effect of having response teams. Potential crisis recognition is the first step in responding to a disaster.

QUESTION NO: 1031

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?

A. Review and evaluate the business continuity plan for adequacy
B. Perform a full simulation of the business continuity plan
C. Train and educate employees regarding the business continuity plan
D. Notify critical contacts in the business continuity plan

Answer: A

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 NO: 1032

Integrating business continuity planning (BCP) into an IT project aids in:

A. the retrofitting of the business continuity requirements.
B. the development of a more comprehensive set of requirements.
C. the development of a transaction flowchart.
D. ensuring the application meets the user's needs.

Answer: B

Explanation:

Integrating business continuity planning (BCP) into the development process ensures complete coverage of the requirements through each phase of the project. Retrofitting of the business continuity plan's requirements occurs when BCP is not integrating into the development methodology. Transaction flowcharts aid in analyzing an application's controls. A business continuity plan will not directly address the detailed processing needs of the users.

QUESTION NO: 1033 CORRECT TEXT

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:

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

Explanation:

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

QUESTION NO: 1034

The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

A. duration of the outage.
B. type of outage.
C. probability of the outage.
D. cause of the outage.

Answer: A
Explanation:
The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.

QUESTION NO: 1035

An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?

A. Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
B. Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
C. Review the methodology adopted by the organization in choosing the service provider.
D. Review the accreditation of the third-party service provider's staff.

Answer: A
Explanation:
Reviewing whether the service provider's business continuity plan (BCP) process is aligned with the organization's BCP and contractual obligations is the correct answer since an adverse effect or disruption to the business of the service provider has a direct bearing on the organization and its customers. Reviewing whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster is not the correct answer since the presence of penalty clauses, although an essential element of a SLA, is not a primary concern. Choices C and D are possible concerns, but of lesser importance.

QUESTION NO: 1036

An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

A. alignment of the BCP with industry best practices.
B. results of business continuity tests performed by IS and end-user personnel.
C. off-site facility, its contents, security and environmental controls.
D. annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Answer: B

Explanation:

The effectiveness of the business continuity plan (BCP) can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives. All other choices do not provide the assurance of the effectiveness of the BCP.

QUESTION NO: 1037

To optimize an organization's business contingency plan (BCP), an IS auditor should

recommend conducting a business impact analysis (BIA) in order to determine:

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

Answer: C

Explanation:

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

QUESTION NO: 1038

A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

A. The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
B. The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
C. The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
D. The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

Answer: B
Explanation:
It is a common mistake to use scenario planning for business continuity. The problem is that it is impossible to plan and document actions for every possible scenario. Planning for just selected scenarios denies the fact that even improbable events can cause an organization to break down. Best practice planning addresses the four possible areas of impact in a disaster: premises, people, systems, and suppliers and other dependencies. All scenarios can be reduced to these four categories and can be handled simultaneously. There are very few special scenarios which justify an additional separate analysis, it is a good idea to use best practices and external advice for such an important topic, especially since knowledge of the right level of preparedness and the judgment about adequacy of the measures taken is not available in every organization. The recovery time objectives (RTOs) are based on the essential business processes required to ensure the organization's survival, therefore it would be inappropriate for them to be based on IT capabilities. Best practice guidelines recommend having 20%-40% of normal capacity available at an emergency site; therefore, a value of 50% would not be a problem if there are no additional factors.

QUESTION NO: 1039

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?

A. Full-scale test with relocation of all departments, including IT, to the contingency site
B. Walk-through test of a series of predefined scenarios with all critical personnel involved
C. IT disaster recovery test with business departments involved in testing the critical applications
D. Functional test of a scenario with limited IT involvement

Answer: D
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.

Topic 8, Mixed Questions

QUESTION NO: 1040

Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

A. it improves security at a cost in functionality.
B. it improves functionality at a cost in security.
C. it improves security at a cost in system performance.
D. it improves performance at a cost in functionality.
E. None of the choices.

Answer: A
Explanation:

"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality. This is a good approach if you have lots of security threats. On the other hand., ""Everything not explicitly forbidden is
permitted"" (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non- existent or negligible."

QUESTION NO: 1041

Default permit is only a good approach in an environment where:

A. security threats are non-existent or negligible.
B. security threats are non-negligible.
C. security threats are serious and severe.
D. users are trained.
E. None of the choices.

Answer: A

Explanation:

"Everything not explicitly permitted is forbidden (default deny) improves security at a cost in functionality. This is a good approach if you have lots of security threats. On the other hand., ""Everything not explicitly forbidden is
permitted"" (default permit) allows greater functionality by sacrificing security. This is only a good approach in an environment where security threats are non- existent or negligible."

QUESTION NO: 1042

Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:

A. most privilege
B. full privilege
C. least privilege
D. null privilege
E. None of the choices.

Answer: C
Explanation:

There are two different approaches to security in computing. One focuses mainly on external threats, and generally treats the computer system itself as a trusted system. The other regards the computer system itself as largely an untrusted system, and redesigns it to make it more secure in a number of ways.
This technique enforces the principle of least privilege to great extent, where an entity has only the privileges that are needed for its function.

QUESTION NO: 1043

Which of the following refers to the proving of mathematical theorems by a computer program?

A. Analytical theorem proving
B. Automated technology proving
C. Automated theorem processing
D. Automated theorem proving
E. None of the choices.

Answer: D
Explanation:

Automated theorem proving (ATP) is the proving of mathematical theorems by a computer program. Depending on the underlying logic, the problem of deciding the validity of a theorem varies from trivial to impossible. Commercial use of automated theorem proving is mostly concentrated in integrated circuit design and verification.

QUESTION NO: 1044

"Which of the following BEST describes the concept of ""defense in depth""?"

A. more than one subsystem needs to be compromised to compromise the security of the system and the information it holds.
B. multiple firewalls are implemented.
C. multiple firewalls and multiple network OS are implemented.
D. intrusion detection and firewall filtering are required.
E. None of the choices.

Answer: A
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 NO: 1045

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

A. ""fail insecure"""
B. ""fail secure"""
C. ""react to attack"""
D. ""react to failure"""
E. None of the choices.

Answer: B
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 NO: 1046

Security should ALWAYS be an all or nothing issue.

A. True
B. True for trusted systems only
C. True for untrusted systems only
D. False
E. None of the choices.

Answer: D
Explanation:

Security should not be an all or nothing issue. The designers and operators of systems should assume that security breaches are inevitable in the long term. Full audit trails should be kept of system activity, so that when a security breach occurs, the mechanism and extent of the breach can be determined.

QUESTION NO: 1047

The 'trusted systems' approach has been predominant in the design of:

A. many earlier Microsoft OS products
B. the IBM AS/400 series
C. the SUN Solaris series
D. most OS products in the market
E. None of the choices.

Answer: A
Explanation:

The 'trusted systems' approach has been predominant in the design of many Microsoft OS products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use'.

QUESTION NO: 1048

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

A. exploit
B. patch
C. quick fix
D. service pack
E. malware

F. None of the choices.

Answer: A
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 NO: 1049

Codes from exploit programs are frequently reused in:

A. trojan horses only.
B. computer viruses only.
C. OS patchers.
D. eavedroppers.
E. trojan horses and computer viruses.
F. None of the choices.

Answer: E
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 NO: 1050

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

A. True
B. False

Answer: B
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 NO: 1051

TEMPEST is a hardware for which of the following purposes?

A. Eavedropping
B. Social engineering
C. Virus scanning
D. Firewalling
E. None of the choices.

Answer: A
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 NO: 1052

Human error is being HEAVILY relied upon on by which of the following types of attack?

A. Eavedropping
B. DoS
C. DDoS
D. ATP
E. Social Engineering
F. None of the choices.

Answer: E
Explanation:

QUESTION NO: 1053

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?

A. Eavedropping
B. DoS
C. DDoS
D. ATP
E. Social Engineering
F. None of the choices.

Answer: C
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 NO: 1054

Attack amplifier is often being HEAVILY relied upon on by which of the following types of attack?

A. Packet dropping
B. ToS
C. DDoS
D. ATP
E. Wiretapping
F. None of the choices.

Answer: C
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 though 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 NO: 1055

Back Orifice is an example of:

A. a virus.
B. a legitimate remote control software.
C. a backdoor that takes the form of an installed program.
D. an eavedropper.
E. None of the choices.

Answer: C

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 NO: 1056

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)?

A. rootkits
B. virus
C. trojan
D. tripwire
E. None of the choices.

Answer: A

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 NO: 1057

Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

A. Direct access attacks
B. Indirect access attacks
C. Port attack
D. Window attack
E. Social attack
F. None of the choices.

Answer: A

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 NO: 1058

Which of the following types of attack almost always requires physical access to the targets?

A. Direct access attack
B. Wireless attack
C. Port attack
D. Window attack
E. System attack
F. None of the choices.

Answer: A
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 NO: 1059

Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

A. key pair
B. Oakley
C. certificate
D. 3-DES
E. one-time pad
F. None of the choices.

Answer: E
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 NO: 1060

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?

A. Blowfish
B. Tripwire
C. certificate
D. DES
E. one-time pad
F. None of the choices.

Answer: E
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 NO: 1061

Why is one-time pad not always preferable for encryption (choose all that apply):

A. it is difficult to use securely.
B. it is highly inconvenient to use.
C. it requires licensing fee.
D. it requires internet connectivity.
E. it is Microsoft only.
F. None of the choices.

Answer: A,B
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 NO: 1062

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

A. keeping your systems up to date using a security scanner.
B. hiring competent people responsible for security to scan and update your systems.
C. using multiple firewalls.
D. using multiple firewalls and IDS.
E. None of the choices.

Answer: A,B
Explanation:

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

QUESTION NO: 1063

Which of the following measures can protect systems files and data, respectively?

A. User account access controls and cryptography
B. User account access controls and firewall
C. User account access controls and IPS
D. IDS and cryptography
E. Firewall and cryptography
F. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1064

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

A. Firewall
B. IDS
C. IPS
D. Hardened OS
E. Tripwire
F. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1065

Which of the following are designed to detect network attacks in progress and assist in post-attack forensics?

A. Intrusion Detection Systems
B. Audit trails
C. System logs
D. Tripwire
E. None of the choices.

Answer: A
Explanation:

Intrusion Detection Systems are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

QUESTION NO: 1066

"Nowadays, computer security comprises mainly "preventive"" measures."

A. True

B. True only for trusted networks
C. True only for untrusted networks
D. False
E. None of the choices.

Answer: A
Explanation:

"Nowadays, computer security comprises mainly ""preventive"" measures, like firewalls or an Exit Procedure. A firewall can be defined as a way of filtering network data between a host or a network and another network and is normally implemented as software running on the machine or as physical integrated hardware."

QUESTION NO: 1067

The majority of software vulnerabilities result from a few known kinds of coding defects, such as (choose all that apply):

A. buffer overflows
B. format string vulnerabilities
C. integer overflow
D. code injection
E. command injection
F. None of the choices.

Answer: A,B,C,D,E
Explanation:

The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common
languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

QUESTION NO: 1068

ALL computer programming languages are vulnerable to command injection attack.

A. True
B. False

Answer: B

Explanation:

The majority of software vulnerabilities result from a few known kinds of coding defects. Common software defects include buffer overflows, format string vulnerabilities, integer overflow, and code/command injection. Some common
languages such as C and C++ are vulnerable to all of these defects. Languages such as Java are immune to some of these defects but are still prone to code/ command injection and other software defects which lead to software vulnerabilities.

QUESTION NO: 1069

Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

A. buffer overflow
B. format string vulnerabilities
C. integer misappropriation
D. code injection
E. None of the choices.

Answer: A
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 NO: 1070

Buffer overflow aims primarily at corrupting:

A. system processor
B. network firewall
C. system memory
D. disk storage
E. None of the choices.

Answer: C
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 NO: 1071

Which of the following measures can effectively minimize the possibility of buffer overflows?

A. Sufficient bounds checking
B. Sufficient memory
C. Sufficient processing capability
D. Sufficient code injection
E. None of the choices.

Answer: A
Explanation:

Buffer overflows may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such,
buffer overflows cause many software vulnerabilities and form the basis of many exploits.
Sufficient bounds checking by either the programmer or the compiler can prevent buffer overflows.

QUESTION NO: 1072

Which of the following types of attack makes use of unfiltered user input as the format string parameter in the printf() function of the C language?

A. buffer overflows
B. format string vulnerabilities
C. integer overflow
D. code injection
E. command injection
F. None of the choices.

Answer: B
Explanation:

Format string attacks are a new class of vulnerabilities recently discovered. It can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write
arbitrary data to arbitrary locations using the %n format token.

QUESTION NO: 1073

Which of the following kinds of function are particularly vulnerable to format string attacks?

A. C functions that perform output formatting
B. C functions that perform integer computation
C. C functions that perform real number subtraction
D. VB functions that perform integer conversion
E. SQL functions that perform string conversion
F. SQL functions that perform text conversion

Answer: A
Explanation:

Format string attacks are a new class of vulnerabilities recently discovered. It can be used to crash a program or to execute harmful code. The problem stems from the use of unfiltered user input as the format string parameter in certain C functions that perform formatting, such as printf(). A malicious user may use the %s and %x format tokens, among others, to print data from the stack or possibly other locations in memory. One may also write arbitrary data to arbitrary locations using the %n format token.

QUESTION NO: 1074

Integer overflow occurs primarily with:

A. string formatting
B. debug operations
C. output formatting
D. input verifications
E. arithmetic operations
F. None of the choices.

Answer: E
Explanation:

An integer overflow occurs when an arithmetic operation attempts to create a numeric value that is larger than can be represented within the available storage space. On some processors the result saturates - once the maximum value is reached attempts to make it larger simply return the maximum result.

QUESTION NO: 1075

Which of the following types of attack works by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs?

A. format string vulnerabilities
B. integer overflow
C. code injection
D. command injection
E. None of the choices.

Answer: C
Explanation:

Code injection is a technique to introduce code into a computer program or system by taking advantage of the unenforced and unchecked assumptions the system makes about its inputs.

QUESTION NO: 1076

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?

A. ILD&P
B. ICT&P
C. ILP&C
D. ILR&D
E. None of the choices.

Answer: A
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 NO: 1077

Network ILD&P are typically installed:

A. on the organization's internal network connection.
B. on the organization's internet network connection.
C. on each end user stations.
D. on the firewall.

E. None of the choices.

Answer: B
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 NO: 1078

Host Based ILD&P primarily addresses the issue of:

A. information integrity
B. information accuracy
C. information validity
D. information leakage
E. None of the choices.

Answer: D
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 NO: 1079

Software is considered malware based on:

A. the intent of the creator.
B. its particular features.
C. its location.
D. its compatibility.
E. None of the choices.

Answer: A

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 NO: 1080

Which of the following are valid examples of Malware (choose all that apply):

A. viruses
B. worms
C. trojan horses
D. spyware
E. All of the above

Answer: E

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 NO: 1081

Which of the following refers to any program that invites the user to run it but conceals a harmful or malicious payload?

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits
F. None of the choices.

Answer: C

Explanation:

QUESTION NO: 1082

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.

A Trojan horse's payload would almost always take damaging effect immediately.

A. True
B. False

Answer: B
Explanation:

Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to immediate yet undesirable effects, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals.

QUESTION NO: 1083

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

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits
F. backdoor
G. None of the choices.

Answer: E
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 NO: 1084

Which of the following refers to a method of bypassing normal system authentication procedures?

A. virus
B. worm
C. trojan horse
D. spyware
E. rootkits
F. backdoor
G. None of the choices.

Answer: F
Explanation:

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

QUESTION NO: 1085

To install backdoors, hackers generally prefer to use:

A. either Trojan horse or computer worm.
B. either Tripwire or computer virus.
C. either eavedropper or computer worm.
D. either Trojan horse or eavedropper.
E. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1086

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

A. wormnets
B. trojannets
C. spynets
D. botnets
E. rootnets
F. backdoor

Answer: D
Explanation:

In order to coordinate the activity of many infected computers, attackers ave used coordinating systems known as botnets. In a botnet, the malware or malbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously.

QUESTION NO: 1087

In a botnet, malbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

A. Chat system
B. SMS system
C. Email system
D. Log system
E. Kernel system
F. None of the choices.

Answer: A
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 malbot logs in to an Internet Relay Chat channel or other chat system. The
attacker can then give instructions to all the infected systems simultaneously.

QUESTION NO: 1088

Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

A. System patcher
B. Porn dialer
C. War dialer

D. T1 dialer
E. T3 dialer
F. None of the choices.

Answer: B
Explanation:

One way of stealing money from infected PC owner is to take control of the modem and dial an expensive toll call. Dialer such as porn dialer software dials up a premium-rate telephone number and leave the line open, charging the
toll to the infected user.

QUESTION NO: 1089

Which of the following is an oft-cited cause of vulnerability of networks?

A. software monoculture
B. software diversification
C. single line of defense
D. multiple DMZ
E. None of the choices.

Answer: A
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 NO: 1090

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

A. poorer performance.
B. poor scalability.
C. weak infrastructure.
D. high costs in terms of training and maintenance.
E. None of the choices.

Answer: D
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 NO: 1091

Which of the following may be deployed in a network as lower cost surveillance and early-warning tools?

A. Honeypots
B. Hardware IPSs
C. Hardware IDSs
D. Botnets
E. Stateful inspection firewalls
F. Stateful logging facilities
G. None of the choices.

Answer: A
Explanation:

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques.

QUESTION NO: 1092

All Social Engineering techniques are based on flaws in:

A. human logic.
B. hardware logic.
C. software logic.
D. device logic.
E. group logic.
F. None of the choices.

Answer: A
Explanation:

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access. All Social Engineering techniques are based on flaws in human logic known as cognitive biases. These bias flaws are used in various combinations to create attack techniques.

QUESTION NO: 1093

Relatively speaking, firewalls operated at the application level of the sevenlayer OSI model are:

A. almost always less efficient.
B. almost always less effective.
C. almost always less secure.
D. almost always less costly to setup.
E. None of the choices.

Answer: A
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 NO: 1094

Relatively speaking, firewalls operated at the physical level of the seven-layer OSI model are:

A. almost always less efficient.
B. almost always less effective.
C. almost always less secure.
D. almost always less costly to setup.
E. None of the choices.

Answer: E
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.

QUESTION NO: 1095
Which of the following refers to the act of creating and using an invented scenario to persuade a

target to perform an action?

A. Pretexting
B. Backgrounding
C. Check making
D. Bounce checking
E. None of the choices.

Answer: A
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 NO: 1096

Pretexting is an act of:

A. DoS
B. social engineering
C. eavedropping
D. soft coding
E. hard coding
F. None of the choices.

Answer: B
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 NO: 1097

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

A. Layer 2 through Layer 7
B. Layer 3 through Layer 7
C. Layer 2 through Layer 6
D. Layer 3 through Layer 6
E. Layer 2 through Layer 5

F. None of the choices.

Answer: A

Explanation:

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

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

QUESTION NO: 1098

Squid is an example of:

A. IDS
B. caching proxy
C. security proxy
D. connection proxy
E. dialer
F. None of the choices.

Answer: B

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 NO: 1099

Which of the following types of firewall treats each network frame or packet in isolation?

A. statefull firewall
B. hardware firewall
C. combination firewall
D. packet filtering firewall
E. stateless firewall
F. None of the choices.

Answer: E

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 NO: 1100

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?

A. Local DoS attacks
B. Remote DoS attacks
C. Distributed DoS attacks
D. Local Virus attacks
E. None of the choices.

Answer: A
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 NO: 1101

What is the best defense against Local DoS attacks?

A. patch your systems.
B. run a virus checker.
C. run an anti-spy software.
D. find this program and kill it.
E. None of the choices.

Answer: D
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 NO: 1102

Which of the following are examples of tools for launching Distributed DoS Attack (choose all that apply):

A. TFN
B. TFN2K
C. Trin00

D. Stacheldracht
E. Tripwire

Answer: A,B,C,D
Explanation:

Distributed DoS Attack is a network-based attack from many servers used remotely to send packets. Examples of tools for conducting such attack include TFN, TFN2K, Trin00, Stacheldracht, and variants. The best defense is to make sure all systems patches are up-to-date. Also make sure your firewalls are configured appropriately.

QUESTION NO: 1103

What is the best defense against Distributed DoS Attack?

A. patch your systems.
B. run a virus checker.
C. run an anti-spy software.
D. find the DoS program and kill it.
E. None of the choices.

Answer: A
Explanation:

Distributed DoS Attack is a network-based attack from many servers used remotely to send packets. Examples of tools for conducting such attack include TFN, TFN2K, Trin00, Stacheldracht, and variants. The best defense is to make sure all systems patches are up-to-date. Also make sure your firewalls are configured appropriately.

QUESTION NO: 1104

What is wrong with a Black Box type of intrusion detection system?

A. you cannot patch it
B. you cannot test it
C. you cannot examine its internal workings from outside.
D. you cannot tune it
E. None of the choices.

Answer: C
Explanation:

"An intrusion detection system should to 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"", coz you want to ensure its internal workings are examinable from outside."

QUESTION NO: 1105

Which of the following are often considered as the first defensive line in protecting a typical data and information environment?

A. certificates
B. security token
C. password
D. biometrics
E. None of the choices.

Answer: C
Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password.

QUESTION NO: 1106

Which of the following are the characteristics of a good password?

A. It has mixed-case alphabetic characters, numbers, and symbols.
B. It has mixed-case alphabetic characters and numbers.
C. It has mixed-case alphabetic characters and symbols.
D. It has mixed-case alphabetic characters, numbers, and binary codes.
E. None of the choices.

Answer: A
Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

QUESTION NO: 1107

What is the recommended minimum length of a good password?

A. 6 characters
B. 8 characters
C. 12 characters
D. 18 characters
E. 22 characters
F. None of the choices.

Answer: B
Explanation:

Passwords are the first defensive line in protecting your data and information. Your users need to be made aware of what a password provides them and what can be done with their password. They also need to be made aware of the
things that make up a good password versus a bad password. A good password has mixed-case alphabetic characters, numbers, and symbols. Do use a password that is at least eight or more characters.

QUESTION NO: 1108

Which of the following is a good tool to use to help enforcing the deployment of good passwords?

A. password cracker
B. local DoS attacker
C. network hacker
D. remote windowing tool
E. None of the choices.

Answer: A
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 NO: 1109

Which of the following is a good time frame for making changes to passwords?

A. every 180 to 365 days
B. every 30 to 45 days
C. every 10 to 20 days
D. every 90 to 120 days
E. None of the choices.

Answer: D
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 NO: 1110

You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):

A. 60 - 75 degrees Fahrenheit
B. 10 - 25 degrees Celsius
C. 30 - 45 degrees Fahrenheit
D. 1 - 15 degrees Celsius
E. 20 - 35 degrees Fahrenheit
F. 0 - 5 degrees Celsius

Answer: A,B
Explanation:

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

QUESTION NO: 1111

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

A. 20 - 70 percent.
B. 10 - 70 percent.
C. 10 - 60 percent.
D. 70 - 90 percent.
E. 60 - 80 percent.
F. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1112

A virus typically consists of what major parts (choose all that apply):

A. a mechanism that allows them to infect other files and reproduce" a trigger that activates delivery of a ""payload"""
B. a payload
C. a signature
D. None of the choices.

Answer: A,B,C
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 NO: 1113

Within a virus, which component is responsible for what the virus does to the victim file?

A. the payload
B. the signature
C. the trigger
D. the premium
E. None of the choices.

Answer: A
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 NO: 1114

Which of the following can be thought of as the simplest and almost cheapest type of firewall?

A. stateful firewall
B. hardware firewall
C. PIX firewall
D. packet filter
E. None of the choices.

Answer: D
Explanation:

The simplest and almost cheapest type of firewall is a packet filter that stops messages with inappropriate network addresses. It usually consists of a screening router and a set of rules that accept or reject a message based on information in the message header.

QUESTION NO: 1115

Screening router inspects traffic through examining:

A. message header.
B. virus payload
C. message content
D. attachment type
E. None of the choices.

Answer: A
Explanation:

The simplest and almost cheapest type of firewall is a packet filter that stops messages with inappropriate network addresses. It usually consists of a screening router and a set of rules that accept or reject a message based on information in the message header.

QUESTION NO: 1116

A major portion of what is required to address nonrepudiation is accomplished through the use of:

A. strong methods for authentication and ensuring data validity
B. strong methods for authentication and ensuring data integrity.
C. strong methods for authorization and ensuring data integrity.
D. strong methods for authentication and ensuring data reliability.
E. None of the choices.

Answer: B
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 NO: 1117

Why is it not preferable for a firewall to treat each network frame or packet in isolation?

A. 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.
B. Such a firewall is costly to setup.
C. Such a firewall is too complicated to maintain.
D. Such a firewall is CPU hungry.
E. Such a firewall offers poor compatibility.
F. None of the choices.

Answer: A
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 NO: 1118

Phishing attack works primarily through:

A. email and hyperlinks
B. SMS
C. chat
D. email attachment
E. news
F. file download
G. None of the choices.

Answer: A

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 NO: 1119

Which of the following types of attack often take advantage of curiosity or greed to deliver malware?

A. Gimmes
B. Tripwire
C. Icing
D. Soft coding
E. Pretexting
F. None of the choices.

Answer: A
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 NO: 1120

Gimmes often work through:

A. SMS
B. IRC chat
C. email attachment
D. news
E. file download
F. None of the choices.

Answer: C
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 NO: 1121

Talking about biometric authentication, physical characteristics typically include (choose all that apply):

A. fingerprints
B. eye retinas
C. irises
D. facial patterns
E. hand measurements
F. None of the choices.

Answer: A,B,C,D,E
Explanation:

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

QUESTION NO: 1122

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

A. Voice
B. Finger measurement
C. Body measurement
D. Signature
E. None of the choices.

Answer: A
Explanation:

Biometric authentication refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes.
Physical characteristics include fingerprints, eye retinas and irises, facial patterns and hand

measurements, while behavioral characteristics include signature, gait and typing patterns. Voice is often considered as a mix of both
physical and behavioral characteristics.

QUESTION NO: 1123

Performance of a biometric measure is usually referred to in terms of (choose all that apply):

A. failure to reject rate
B. false accept rate
C. false reject rate
D. failure to enroll rate
E. None of the choices.

Answer: B,C,D
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 NO: 1124

Talking about biometric measurement, which of the following measures the percent of invalid users who are incorrectly accepted in?

A. failure to reject rate
B. false accept rate
C. false reject rate
D. failure to enroll rate
E. None of the choices.

Answer: B
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 NO: 1125

An accurate biometric system usually exhibits (choose all that apply):

A. low EER
B. low CER
C. high EER
D. high CER
E. None of the choices.

Answer: A,B
Explanation:

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

QUESTION NO: 1126

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?

A. CRC-32
B. CRC-64
C. DES
D. 3DES
E. RC4
F. RC5
G. None of the choices.

Answer: E
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 NO: 1127

As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the CRC- 32 checksum for:

A. integrity.

B. validity.
C. accuracy.
D. confidentiality.
E. None of the choices.

Answer: A
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 NO: 1128

Many WEP systems require a key in a relatively insecure format. What format is this?

A. binary format.
B. hexadecimal format.
C. 128 bit format.
D. 256 bit format.
E. None of the choices.

Answer: B
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 NO: 1129

Wi-Fi Protected Access implements the majority of which IEEE standard?

A. 802.11i
B. 802.11g
C. 802.11x
D. 802.11v
E. None of the choices.

Answer: A

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 NO: 1130

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?

A. SKIP
B. RKIP
C. OKIP
D. EKIP
E. TKIP
F. None of the choices.

Answer: E
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 NO: 1131

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

A. stream cipher
B. block cipher
C. check cipher
D. string cipher
E. None of the choices.

Answer: B
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 NO: 1132

Which of the following typically consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared?

A. honeypot
B. superpot
C. IDS
D. IPS
E. firewall
F. None of the choices.

Answer: A
Explanation:

You may use a honeypot to detect and deflect unauthorized use of your information systems. A typical honeypot consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared for trapping hackers.

QUESTION NO: 1133

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

A. honeymoon
B. honeytrap
C. honeytube
D. honeyd
E. None of the choices.

Answer: D
Explanation:

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

QUESTION NO: 1134

Which of the following are valid choices for the Apache/SSL combination (choose all that apply):

A. the Apache-SSL project
B. third-party SSL patches
C. the mod_ssl module
D. the mod_css module
E. None of the choices.

Answer: A,B,C
Explanation:

On Linux you have Apache which is supposed to be a safer choice of web service. In fact you have several choices for the Apache/SSL combination, such as the Apache-SSL project (www.apache-ssl.org) using third-party SSL patches, or
have Apache compiled with the mod_ssl module.

QUESTION NO: 1135

What would be the major purpose of rootkit?

A. to hide evidence from system administrators.
B. to encrypt files for system administrators.
C. to corrupt files for system administrators.
D. to hijack system sessions.
E. None of the choices.

Answer: A
Explanation:

rootkit originally describes those recompiled Unix tools that would hide any trace of the intruder. You can say that the only purpose of rootkit is to hide evidence from system administrators so there is no way to detect malicious
special privilege access attempts.

QUESTION NO: 1136

Most trojan horse programs are spread through:

A. e-mails.
B. MP3.

C. MS Office.
D. Word template.
E. None of the choices.

Answer: A
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 NO: 1137

The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?

A. e-mails.
B. MP3.
C. MS Office.
D. Word template.
E. None of the choices.

Answer: B
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 NO: 1138

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

A. Keywords logging
B. Keystroke logging
C. Directory logging
D. Password logging
E. None of the choices.

Answer: B

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 NO: 1139

You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?

A. exploit
B. vulnerability
C. both

Answer: B

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 NO: 1140

Which of the following is a rewrite of ipfwadm?

A. ipchains
B. iptables
C. Netfilter
D. ipcook
E. None of the choices.

Answer: A

Explanation:

ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above.
Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

QUESTION NO: 1141

Iptables is based on which of the following frameworks?

A. Netfilter
B. NetDoom
C. NetCheck
D. NetSecure
E. None of the choices.

Answer: A
Explanation:

ipchains is a free software based firewall running on earlier Linux. It is a rewrite of ipfwadm but is superseded by iptables in Linux 2.4 and above.

Iptables controls the packet filtering and NAT components within the Linux kernel. It is based on Netfilter, a framework which provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.

QUESTION NO: 1142

Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?

A. datagram scanning
B. access lists
C. stateful inspection
D. state checking
E. link progressing
F. None of the choices.

Answer: B
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 NO: 1143

Which of the following correctly describe the potential problem of deploying Wi-Fi Protected Access to secure your wireless network?

A. potential compatibility problems with wireless network interface cards.
B. potential compatibility problems with wireless access points.
C. potential performance problems with wireless network interface cards.
D. potential performance problems with wireless access points.
E. None of the choices.

Answer: B
Explanation:

Wi-Fi Protected Access (WPA / WPA2) is a class of systems to secure wireless computer networks. It implements the majority of the IEEE 802.11i standard, and is designed to work with all wireless network interface cards (but
not necessarily with first generation wireless access points).

QUESTION NO: 1144

The Federal Information Processing Standards (FIPS) were developed by:

A. the United States Federal government
B. ANSI
C. ISO
D. IEEE
E. IANA
F. None of the choices.

Answer: A
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.

QUESTION NO: 1145

The Federal Information Processing Standards (FIPS) are primarily for use by (choose all that apply):

A. all non-military government agencies

B. US government contractors
C. all military government agencies
D. all private and public colleges in the US
E. None of the choices.

Answer: A,B
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.

QUESTION NO: 1146

Sophisticated database systems provide many layers and types of security, including (choose all that apply):

A. Access control
B. Auditing
C. Encryption
D. Integrity controls
E. Compression controls

Answer: A,B,C,D
Explanation:

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

QUESTION NO: 1147

Which of the following refers to an important procedure when evaluating database security (choose the BEST answer)?

A. performing vulnerability assessments against the database.
B. performing data check against the database.
C. performing dictionary check against the database.

D. performing capacity check against the database system.
E. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1148

Which of the following refers to any authentication protocol that requires two independent ways to establish identity and privileges?

A. Strong-factor authentication
B. Two-factor authentication
C. Dual-password authentication
D. Two-passphrases authentication
E. Dual-keys authentication
F. Rich-factor authentication

Answer: B
Explanation:

Two-factor authentication (T-FA) refers to any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as
the other factor. In fact, using more than one factor is also called strong authentication. On the other hand, using just one factor is considered by some weak authentication.

QUESTION NO: 1149

Common implementations of strong authentication may use which of the following factors in their authentication efforts (choose all that apply):

A. 'something you know'
B. 'something you have'
C. 'something you are'

D. 'something you have done in the past on this same system'
E. 'something you have installed on this same system'
F. None of the choices.

Answer: A,B,C
Explanation:

Two-factor authentication (T-FA) refers to any authentication protocol that requires two independent ways to establish identity and privileges. Common implementations of two-factor authentication use 'something you know' as one of the two factors, and use either 'something you have' or 'something you are' as the other factor. In fact, using more than one factor is also called strong authentication. On the other hand, using just one factor is considered by some weak authentication.

QUESTION NO: 1150

Effective transactional controls are often capable of offering which of the following benefits (choose all that apply):

A. reduced administrative and material costs
B. shortened contract cycle times
C. enhanced procurement decisions
D. diminished legal risk
E. None of the choices.

Answer: A,B,C,D
Explanation:

Transactional systems provide a baseline necessary to measure and monitor contract performance and provide a method for appraising efficiency against possible areas of exposure. Effective transactional controls reduce administrative and material costs, shorten contract cycle times, enhance procurement decisions, and diminish legal risk.

QUESTION NO: 1151

In the context of physical access control, what is known as the process of verifying user identities?

A. Authentication
B. Authorization
C. Accounting
D. Encryption
E. Compression
F. None of the choices.

Answer: A

Explanation:

Authentication is the process of verifying a user's claimed identity. It is based on at least one of these three factors: Something you know, Something you have, or Something you are.

QUESTION NO: 1152

Physical access controls are usually implemented based on which of the following means (choose all that apply):

A. mechanical locks
B. guards
C. operating systems
D. transaction applications
E. None of the choices.

Answer: A,B

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 NO: 1153

Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems (choose all that apply):

A. desktop systems
B. laptop systems
C. handheld PDAs
D. business-critical systems
E. None of the choices.

Answer: D

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 businesscritical
systems.

QUESTION NO: 1154

The technique of rummaging through commercial trash to collect useful business information is known as:

A. Information diving
B. Intelligence diving
C. Identity diving
D. System diving
E. Program diving
F. None of the choices.

Answer: A
Explanation:

Dumpster diving in the form of information diving describes the practice of rummaging through commercial trash to find useful information such as files, letters, memos, passwords ...etc.

QUESTION NO: 1155

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

A. Software audit
B. System audit
C. Application System audit
D. Test audit
E. Mainframe audit
F. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1156

The purpose of a mainframe audit is to provide assurance that (choose all that apply):

A. processes are being implemented as required
B. the mainframe is operating as it should
C. security is strong
D. procedures in place are working
E. procedures in place are updated as needed
F. the OS applications are secured
G. None of the choices.

Answer: A,B,C,D,E
Explanation:

The purpose of a mainframe audit is to provide assurance that processes are being implemented as required, the mainframe is operating as it should, security is strong, and that procedures in place are working and are updated as needed. The auditor may accordingly make recommendations for improvement.
Which of the following types of audit always takes high priority over the others?
A. System audit
B. Application audit
C. Software audit
D. License audit
E. Security server audit
F. None of the choices.
Answer: E
Security server audit always takes high priority because the security administrators who manage this not only have elevated privilege, but also model and create the user passwords. Are proper segregation of duties implemented and
enforced and is technology and procedures in place to make sure there is a continuous and accurate audit trail?

QUESTION NO: 1157

In a security server audit, focus should be placed on (choose all that apply):

A. proper segregation of duties
B. adequate user training
C. continuous and accurate audit trail
D. proper application licensing
E. system stability
F. performance and controls of the system
G. None of the choices.

Answer: A,C

Explanation:

Security server audit always takes high priority because the security administrators who manage this not only have elevated privilege, but also model and create the user passwords. Are proper segregation of duties implemented and
enforced and is technology and procedures in place to make sure there is a continuous and accurate audit trail?

QUESTION NO: 1158

Talking about application system audit, focus should always be placed on:

A. performance and controls of the system
B. the ability to limit unauthorized access and manipulation
C. input of data are processed correctly
D. output of data are processed correctly
E. changes to the system are properly authorized
F. None of the choices.

Answer: A,B,C,D,E
Explanation:

Talking about application system audit, focus should be placed on the performance and controls of the system, its ability to limit unauthorized access and manipulation, that input and output of data are processed correctly on the
system, that any changes to the system are authorized, and that users have access to the system.

QUESTION NO: 1159

A successful risk-based IT audit program should be based on:

A. an effective scoring system.
B. an effective PERT diagram.
C. an effective departmental brainstorm session.
D. an effective organization-wide brainstorm session.
E. an effective yearly budget.
F. None of the choices.

Answer: A
Explanation:

A successful risk-based IT audit program could be based on an effective scoring system. In establishing a scoring system, management should consider all relevant risk factors and avoid subjectivity. Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee.

QUESTION NO: 1160

The use of risk assessment tools for classifying risk factors should be formalized in your IT audit effort through:

A. the use of risk controls.
B. the use of computer assisted functions.
C. using computer assisted audit technology tools.
D. the development of written guidelines.
E. None of the choices.

Answer: D
Explanation:

A successful risk-based IT audit program could be based on an effective scoring system. In establishing a scoring system, management should consider all relevant risk factors and avoid subjectivity. Auditors should develop written guidelines on the use of risk assessment tools and risk factors and review these guidelines with the audit committee.

QUESTION NO: 1161

Which of the following correctly describes the purpose of an Electronic data processing audit?

A. to collect and evaluate evidence of an organization's information systems, practices, and operations.
B. to ensure document validity.
C. to verify data accuracy.
D. to collect and evaluate benefits brought by an organization's information systems to its bottomline.
E. None of the choices.

Answer: A
Explanation:

An Electronic data processing (EDP) audit is an IT audit. It is the process of collecting and evaluating evidence of an organization's information systems, practices, and operations.

QUESTION NO: 1162

What should be done to determine the appropriate level of audit coverage for an organization's IT environment?

A. determine the company's quarterly budget requirement.
B. define an effective assessment methodology.
C. calculate the company's yearly budget requirement.
D. define an effective system upgrade methodology.
E. define an effective network implementation methodology.

Answer: B
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 NO: 1163

IS audits should be selected through a risk analysis process to concentrate on:

A. those areas of greatest risk and opportunity for improvements.
B. those areas of least risk and opportunity for improvements.
C. those areas of the greatest financial value.
D. areas led by the key people of the organization.
E. random events.
F. irregular events.

Answer: A
Explanation:

Audits are typically selected through a risk analysis process to concentrate on those areas of greatest risk and opportunity for improvements.

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

QUESTION NO: 1164

Your final audit report should be issued:

A. after an agreement on the observations is reached.
B. before an agreement on the observations is reached.
C. if an agreement on the observations cannot reached.

D. without mentioning the observations.
E. None of the choices.

Answer: A
Explanation:

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

QUESTION NO: 1165

Well-written risk assessment guidelines for IS auditing should specify which of the following elements at the least (choose all that apply):

A. A maximum length for audit cycles.
B. The timing of risk assessments.
C. Documentation requirements.
D. Guidelines for handling special cases.
E. None of the choices.

Answer: A,B,C,D
Explanation:

A well-written risk assessment guidelines should specify a maximum length for audit cycles based on the risk scores and the timing of risk assessments for each department or activity. There should be documentation requirements to
support scoring decisions. There should also be guidelines for overriding risk assessments in special cases and the circumstances under which they can be overridden.

QUESTION NO: 1166

The ability of the internal IS audit function to achieve desired objectives depends largely on:

A. the training of audit personnel
B. the background of audit personnel
C. the independence of audit personnel
D. the performance of audit personnel
E. None of the choices.

Answer: C
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 NO: 1167

In-house personnel performing IS audits should posses which of the following knowledge and/or skills (choose 2):

A. information systems knowledge commensurate with the scope of the IT environment in question
B. sufficient analytical skills to determine root cause of deficiencies in question
C. sufficient knowledge on secure system coding
D. sufficient knowledge on secure platform development
E. information systems knowledge commensurate outside of the scope of the IT environment in question

Answer: A,B
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 NO: 1168

A comprehensive IS audit policy should include guidelines detailing what involvement the internal audit team should have?

A. in the development and coding of major OS applications.
B. in the acquisition and maintenance of major WEB applications.
C. in the human resource management cycle of the application development project.
D. in the development, acquisition, conversion, and testing of major applications.
E. None of the choices.

Answer: D
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 NO: 1169

For application acquisitions with significant impacts, participation of your IS audit team should be encouraged:

A. early in the due diligence stage.
B. at the testing stage.
C. at the final approval stage.
D. at the budget preparation stage.
E. None of the choices.

Answer: A
Explanation:

For acquisitions with significant IT impacts, participation of IS audit is often necessary early in the due diligence stage as defined in the audit policy.

QUESTION NO: 1170

Which of the following should be seen as one of the most significant factors considered when determining the frequency of IS audits within your organization?

A. The cost of risk analysis
B. The income generated by the business function
C. Resource allocation strategy
D. The nature and level of risk
E. None of the choices.

Answer: D
Explanation:

You use a risk assessment process to describe and analyze the potential audit risks inherent in a given line of business. You should update such risk assessment at least annually to reflect changes. The level and nature of risk should be the most significant factors to be considered when determining the frequency of audits.

QUESTION NO: 1171

Properly planned risk-based audit programs are often capable of offering which of the following benefits?

A. audit efficiency and effectiveness.
B. audit efficiency only.
C. audit effectiveness only.

D. audit transparency only.
E. audit transparency and effectiveness.
F. None of the choices.

Answer: A
Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

QUESTION NO: 1172

The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

A. the target's management hands-on involvement.
B. the target's location.
C. the target's size and complexity.
D. the target's budget.
E. the target's head count.
F. None of the choices.

Answer: C
Explanation:

Properly planned risk-based audit programs shall increase audit efficiency and effectiveness. The sophistication and formality of this kind of audit do vary a lot depending on the target's size and complexity.

QUESTION NO: 1173

Which of the following is one most common way that spyware is distributed?

A. as a trojan horse.
B. as a virus.
C. as an Adware.
D. as a device driver.
E. as a macro.
F. None of the choices.

Answer: A

Explanation: One of the most common ways that spyware is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads off the Web or a peer-to-peer file-trading network. When the user installs the software, the spyware is installed alongside.

QUESTION NO: 1174

Which of the following is not a good tactic to use against hackers?

A. Enticement
B. Entrapment

Answer: B

Explanation: Enticement occurs after somebody has gained unlawful access to a system and then subsequently lured to a honey pot. Entrapment encourages the commitment of unlawful access. The latter is not a good tactic to use as it involves encouraging someone to commit a crime.

QUESTION NO: 1175

Creating which of the following is how a hacker can insure his ability to return to the hacked system at will?

A. rootsec
B. checksum
C. CRC
D. backdoors
E. None of the choices.

Answer: D

Explanation: A backdoor refers to a generally undocumented means of getting into a system, mostly for programming and maintenance/troubleshooting needs. Most real world programs have backdoors. Creating backdoors is how a hacker can insure his ability to return to the hacked system at will.

QUESTION NO: 1176

A trojan horse simply cannot operate autonomously.

A. true
B. false

Answer: A
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 NO: 1177

Which of the following refers to the collection of policies and procedures for implementing controls capable of restricting access to computer software and data files?

A. Binary access control
B. System-level access control
C. Logical access control
D. Physical access control
E. Component access control
F. None of the choices.

Answer: C
Explanation:

Logical access control is about the use of a collection of policies, procedures, and controls to restrict access to computer software and data files.

Such control system should provide reasonable assurance that an organization's objectives are being properly achieved securely and reliably.