



# Isaca

## Exam Questions CISA

Isaca CISA

## About ExamBible

*[Your Partner of IT Exam](#)*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

- (Topic 1)

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.

#### NEW QUESTION 2

- (Topic 1)

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.

#### NEW QUESTION 3

- (Topic 1)

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.

#### NEW QUESTION 4

- (Topic 1)

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

- A. cold sit
- B. warm sit
- C. dial-up sit
- D. duplicate processing facilit

**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.

#### NEW QUESTION 5

- (Topic 1)

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 schem
- B. defining security and integrity check
- C. liaising with users in developing data mode
- D. mapping data model with the internal schem

**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.

#### NEW QUESTION 6

- (Topic 1)

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

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

**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.

#### NEW QUESTION 7

- (Topic 1)

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.

#### NEW QUESTION 8

- (Topic 1)

The use of a GANTT chart can:

- A. aid in scheduling project task
- B. determine project checkpoint
- C. ensure documentation standard
- 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.

#### NEW QUESTION 9

- (Topic 1)

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.

#### NEW QUESTION 10

- (Topic 1)

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 administratio

**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.

#### NEW QUESTION 10

- (Topic 1)

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.

#### NEW QUESTION 14

- (Topic 1)

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

- A. development and implementation of an information security standards manua
- B. performance of a comprehensive security control review by the IS audito
- C. adoption of a corporate information security policy statemen
- D. purchase of security access control softwar

**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.

#### NEW QUESTION 16

- (Topic 1)

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

- A. logic bom
- B. stealth viru
- C. trojan hors
- D. polymorphic viru

**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.

#### NEW QUESTION 20

- (Topic 1)

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.

#### NEW QUESTION 22

- (Topic 1)

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.

#### NEW QUESTION 25

- (Topic 1)

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.

#### NEW QUESTION 26

- (Topic 1)

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.

#### NEW QUESTION 30

- (Topic 1)

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.

#### NEW QUESTION 32

- (Topic 1)

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.

#### NEW QUESTION 37

- (Topic 1)

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.

**NEW QUESTION 39**

- (Topic 1)

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.

**NEW QUESTION 40**

- (Topic 1)

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.

**NEW QUESTION 45**

- (Topic 1)

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 decrease
- B. Risk of unauthorized and untraceable changes to the database increase
- C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increase
- D. Risk of unauthorized and untraceable changes to the database decrease

**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.

**NEW QUESTION 48**

- (Topic 1)

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.

**NEW QUESTION 53**

- (Topic 1)

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.

**NEW QUESTION 56**

- (Topic 1)

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.

**NEW QUESTION 61**

- (Topic 1)

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 ke
- B. Upon receiving the data, the recipient can decrypt the data using the sender's public ke
- C. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public ke
- D. Upon receiving the data, the recipient can decrypt the data using the recipient's public ke
- E. 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 content
- F. Upon receiving the data, the recipient can independently create i
- G. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public ke
- H. Upon receiving the data, the recipient can decrypt the data using the recipient's private ke

**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.

**NEW QUESTION 64**

- (Topic 1)

What is the key distinction between encryption and hashing algorithms?

- A. Hashing algorithms ensure data confidentialit
- B. Hashing algorithms are irreversibl
- C. Encryption algorithms ensure data integrit
- D. Encryption algorithms are not irreversibl

**Answer: B**

**Explanation:**

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

**NEW QUESTION 65**

- (Topic 1)

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).

**NEW QUESTION 68**

- (Topic 1)

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.

**NEW QUESTION 71**

- (Topic 1)

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.

**NEW QUESTION 75**

- (Topic 1)

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.

**NEW QUESTION 77**

- (Topic 1)

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.

**NEW QUESTION 82**

- (Topic 1)

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.

**NEW QUESTION 85**

- (Topic 1)

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.

#### NEW QUESTION 89

- (Topic 1)

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.

#### NEW QUESTION 93

- (Topic 1)

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
- C. Furthermore, the IS auditor should create formal documented policies to be implemented
- D. The auditor should at least document the informal standards and policies, and test for compliance
- E. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented
- F. The auditor should at least document the informal standards and policies, and test for compliance
- G. 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.

#### NEW QUESTION 96

- (Topic 1)

\_\_\_\_\_ (fill in the blank) is/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.

#### NEW QUESTION 97

- (Topic 1)

\_\_\_\_\_ 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.

#### NEW QUESTION 100

- (Topic 1)

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.

#### NEW QUESTION 104

- (Topic 1)

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.

#### NEW QUESTION 107

- (Topic 1)

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.

#### NEW QUESTION 109

- (Topic 1)

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.

#### NEW QUESTION 114

- (Topic 1)

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).

#### NEW QUESTION 116

- (Topic 1)

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.

#### NEW QUESTION 118

- (Topic 1)

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.

**NEW QUESTION 123**

- (Topic 1)

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 control
- 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.

**NEW QUESTION 127**

- (Topic 1)

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.

**NEW QUESTION 129**

- (Topic 1)

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.

**NEW QUESTION 132**

- (Topic 1)

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.

**NEW QUESTION 133**

- (Topic 1)

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.

**NEW QUESTION 136**

- (Topic 1)

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.

#### NEW QUESTION 141

- (Topic 1)

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.

#### NEW QUESTION 144

- (Topic 1)

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.

#### NEW QUESTION 146

- (Topic 1)

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.

#### NEW QUESTION 151

- (Topic 1)

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.

#### NEW QUESTION 153

- (Topic 1)

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.

**NEW QUESTION 156**

- (Topic 1)

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.

**NEW QUESTION 157**

- (Topic 1)

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.

**NEW QUESTION 162**

- (Topic 1)

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.

**NEW QUESTION 165**

- (Topic 1)

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.

**NEW QUESTION 170**

- (Topic 1)

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.

**NEW QUESTION 174**

- (Topic 1)

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.

#### NEW QUESTION 175

- (Topic 1)

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.

#### NEW QUESTION 177

- (Topic 1)

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.

#### NEW QUESTION 178

- (Topic 1)

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.

#### NEW QUESTION 179

- (Topic 1)

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.

#### NEW QUESTION 183

- (Topic 1)

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.

**NEW QUESTION 186**

- (Topic 1)

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.

**NEW QUESTION 187**

- (Topic 1)

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.

**NEW QUESTION 190**

- (Topic 1)

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.

**NEW QUESTION 192**

- (Topic 1)

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.

**NEW QUESTION 197**

- (Topic 1)

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.

#### NEW QUESTION 202

- (Topic 1)

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.

#### NEW QUESTION 207

- (Topic 1)

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.

#### NEW QUESTION 208

- (Topic 1)

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.

#### NEW QUESTION 209

- (Topic 1)

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.

#### NEW QUESTION 211

- (Topic 2)

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.

#### NEW QUESTION 213

- (Topic 2)

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 activities
- 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.

#### NEW QUESTION 217

- (Topic 2)

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 system

**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 often does require an IS auditor to collect evidence on system reliability while processing is taking place. Choice B is incorrect since an IS auditor normally would review and follow up only on material deficiencies or errors detected. Choice D is incorrect since the use of continuous audit techniques depends on the complexity of an organization's computer systems.

#### NEW QUESTION 218

- (Topic 2)

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.

#### NEW QUESTION 219

- (Topic 2)

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 engagement
- 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.

#### NEW QUESTION 220

- (Topic 2)

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 asset
- D. the threats/vulnerabilities affecting the asset

**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.

**NEW QUESTION 224**

- (Topic 2)

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

- A. address audit objective
- B. collect sufficient evidenc
- C. specify appropriate test
- D. minimize audit resource

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

**NEW QUESTION 225**

- (Topic 2)

An IS auditor evaluating logical access controls should FIRST:

- A. document the controls applied to the potential access paths to the syste
- B. test controls over the access paths to determine if they are functiona
- C. evaluate the security environment in relation to written policies and practices
- D. obtain an understanding of the security risks to information processin

**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 and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

**NEW QUESTION 227**

- (Topic 2)

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.

**NEW QUESTION 232**

- (Topic 2)

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 desktop
- 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 detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

#### NEW QUESTION 235

- (Topic 2)

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.

#### NEW QUESTION 239

- (Topic 2)

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 time-intensive. 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.

#### NEW QUESTION 242

- (Topic 2)

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.

#### NEW QUESTION 247

- (Topic 2)

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.

#### NEW QUESTION 251

- (Topic 2)

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 independenc
- C. technical competenc
- D. professional competenc

**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.

#### NEW QUESTION 252

- (Topic 2)

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

- A. understand the business proces
- B. comply with auditing standard
- C. identify control weaknes
- D. plan substantive testin

**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.

#### NEW QUESTION 253

- (Topic 2)

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 issue
- B. gain agreement on the finding
- C. receive feedback on the adequacy of the audit procedure
- D. test the structure of the final presentatio

**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.

#### NEW QUESTION 254

- (Topic 2)

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.

#### NEW QUESTION 259

- (Topic 2)

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 not identify duplicate records. An integrated test facility (ITF) allows the IS auditor to test transactions through the production system, but would not compare records to identify duplicates.

#### NEW QUESTION 261

- (Topic 2)

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.

#### NEW QUESTION 262

- (Topic 2)

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 owner

**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.

#### NEW QUESTION 267

- (Topic 2)

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

- A. audit committee
- B. auditee's management
- 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.

#### NEW QUESTION 270

- (Topic 2)

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 the degree to which line managers assume responsibility for controls. Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

#### NEW QUESTION 274

- (Topic 2)



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, all of which are representations of broad stakeholder involvement. Choices B, C and D are attributes of a traditional audit approach.

#### NEW QUESTION 278

- (Topic 3)

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

- A. whether IT processes support business requirement
- 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.

#### NEW QUESTION 280

- (Topic 3)

An IS steering committee should:

- A. include a mix of members from different departments and staff level
- B. ensure that IS security policies and procedures have been executed properly
- C. have formal terms of reference and maintain minutes of its meeting
- 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.

#### NEW QUESTION 284

- (Topic 3)

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.

#### NEW QUESTION 288

- (Topic 3)

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 strategies and objectives, and that the strategy is aligned with business strategy. Choice A is incorrect because it is the IT strategy that extends the organizational objectives, not the opposite. IT governance is not an isolated discipline; it must become an integral part of the overall enterprise governance.

#### NEW QUESTION 290

- (Topic 3)

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.

#### NEW QUESTION 291

- (Topic 3)

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

#### NEW QUESTION 292

- (Topic 3)

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.

#### NEW QUESTION 297

- (Topic 3)

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.

#### NEW QUESTION 302

- (Topic 3)

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.

#### NEW QUESTION 305

- (Topic 3)

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 need
- B. plans are consistent with management strateg
- C. uses its equipment and personnel efficiently and effectiveI
- D. has sufficient excess capacity to respond to changing direction

**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.

#### NEW QUESTION 308

- (Topic 3)

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 objective
- B. actions to reduce hardware procurement cos
- C. a listing of approved suppliers of IT contract resource
- D. a description of the technical architecture for the organization's network perimeter securit

**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 to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail of a specific technical architecture.

#### NEW QUESTION 312

- (Topic 3)

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 whol
- B. are more likely to be derived as a result of a risk assessmen
- C. will not conflict with overall corporate polic
- D. ensure consistency across the organizatio

**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.

#### NEW QUESTION 313

- (Topic 3)

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 informatio
- B. information security is not critical to all function
- C. IS audit should provide security training to the employee
- D. the audit finding will cause management to provide continuous training to staf

**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.

#### NEW QUESTION 314

- (Topic 3)

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.

#### NEW QUESTION 315

- (Topic 3)

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

- A. recover
- B. retentio
- C. rebuildin
- D. reus

**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 official form of classic 'paper' makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

#### NEW QUESTION 319

- (Topic 3)

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 will often set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

#### NEW QUESTION 324

- (Topic 3)

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.

#### NEW QUESTION 329

- (Topic 3)

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 procedure
- 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.

#### NEW QUESTION 333

- (Topic 3)

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.

#### NEW QUESTION 334

- (Topic 3)

To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

- A. project management tool
- 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.

#### NEW QUESTION 337

- (Topic 3)

In the context of effective information security governance, the primary objective of value delivery is to:

- A. optimize security investments in support of business objective
- 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.

#### NEW QUESTION 339

- (Topic 3)

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.

**NEW QUESTION 342**

- (Topic 3)

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.

**NEW QUESTION 347**

- (Topic 3)

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.

**NEW QUESTION 352**

- (Topic 3)

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 the loss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionality in this context is a vulnerability.

**NEW QUESTION 355**

- (Topic 3)

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 recommendation
- B. enforcement of the management of security risk
- C. implementation of the chief information security officer's (CISO) recommendation
- 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.

**NEW QUESTION 360**

- (Topic 4)

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 complete
- 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.

#### NEW QUESTION 363

- (Topic 4)

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 tool

**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.

#### NEW QUESTION 365

- (Topic 4)

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.

#### NEW QUESTION 370

- (Topic 4)

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.

#### NEW QUESTION 371

- (Topic 4)

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 that the earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

**NEW QUESTION 373**

- (Topic 4)

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 on the critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

**NEW QUESTION 375**

- (Topic 4)

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.

**NEW QUESTION 379**

- (Topic 4)

An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

- A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plan
- 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 management practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

**NEW QUESTION 382**

- (Topic 4)

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 IT governance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

#### NEW QUESTION 386

- (Topic 4)

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.

#### NEW QUESTION 387

- (Topic 4)

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 (SDPT)
- 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 for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

#### NEW QUESTION 389

- (Topic 4)

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 issue
- D. recommend that the project manager reallocate test resources to resolve the issue

**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 choices might be appropriate only after the risks have been assessed.

#### NEW QUESTION 391

- (Topic 4)

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 for dependencies between tasks, while overestimating the completion percentage for tasks underway (80:20 rule). The calculation based on remaining budget does not take into account the speed at which the project has been progressing.

#### NEW QUESTION 396

- (Topic 4)

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

- A. Application programmers are implementing changes to production program
- B. Application programmers are implementing changes to test program
- C. Operations support staff are implementing changes to batch schedule
- D. Database administrators are implementing changes to data structure

**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 will affect the scheduling of the batches only; it does not impact the live data. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

#### NEW QUESTION 398

- (Topic 4)

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 be ensured by using digital signatures.

#### NEW QUESTION 400

- (Topic 4)

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.

#### NEW QUESTION 404

- (Topic 4)

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.

#### NEW QUESTION 409

- (Topic 4)

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 is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

#### NEW QUESTION 410

- (Topic 4)

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, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

#### NEW QUESTION 413

- (Topic 4)

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 goal
- C. a documented process
- D. a process tailored to specific project

**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.

#### NEW QUESTION 415

- (Topic 4)

Ideally, stress testing should be carried out in a:

- A. test environment using test data
- B. production environment using live workload
- C. test environment using live workload
- 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 B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

#### NEW QUESTION 418

- (Topic 4)

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.

#### NEW QUESTION 423

- (Topic 4)

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 error

**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.

#### NEW QUESTION 424

- (Topic 4)

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.

#### NEW QUESTION 426

- (Topic 4)

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 maintainanc
- B. improper documentation of testin
- C. inadequate functional testin
- D. delays in problem resolutio

**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.

#### NEW QUESTION 431

- (Topic 4)

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 overflo
- B. brute force attac
- C. distributed denial-of-service attac
- D. war dialing attac

**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.

#### NEW QUESTION 436

- (Topic 4)

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 are advantages of the bottom-up approach to system testing.

#### NEW QUESTION 441

- (Topic 4)

During the system testing phase of an application development project the IS auditor should review the:

- A. conceptual design specification
- B. vendor contract
- C. error report
- D. program change request

**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. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

#### NEW QUESTION 442

- (Topic 4)

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 path
- 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.

#### NEW QUESTION 444

- (Topic 4)

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.

#### NEW QUESTION 445

- (Topic 4)

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.

#### NEW QUESTION 446

- (Topic 4)

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.

#### NEW QUESTION 451

- (Topic 4)

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 form
- B. gross payroll should be recalculated manually
- C. checks (cheques) should be compared to input form
- D. checks (cheques) should be reconciled with output report

**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 is the best mechanism of verifying data accuracy. Recalculating gross payroll manually would only verify whether the processing is correct and not the data accuracy of inputs. Comparing checks (cheques) to input forms is not feasible as checks (cheques) have the processed information and input forms have the input data. Reconciling checks (cheques) with output reports only confirms that checks (cheques) have been issued as per output reports.

#### NEW QUESTION 452

- (Topic 4)

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.

#### NEW QUESTION 455

- (Topic 4)

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 to verify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

#### NEW QUESTION 456



- (Topic 4)

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

- A. secure communication
- B. improved performanc
- C. efficient interfacin
- D. enhanced documentatio

**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.

#### NEW QUESTION 461

- (Topic 4)

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 and D are possible considerations but would not be the most important.

#### NEW QUESTION 466

- (Topic 4)

An IS auditor performing an application maintenance audit would review the log of program changes for the:

- A. authorization of program change
- B. creation date of a current object modul
- C. number of program changes actually mad
- D. creation date of a current source progra

**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.

#### NEW QUESTION 467

- (Topic 4)

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 task
- B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old syste
- C. A single implementation is planned, immediately decommissioning the legacy syste
- D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's softwar

**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 the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

#### NEW QUESTION 471

.....

## Relate Links

**100% Pass Your CISA Exam with Exambible Prep Materials**

<https://www.exambible.com/CISA-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>