

# Exam Questions CISA

Isaca CISA

<https://www.2passeasy.com/dumps/CISA/>



#### NEW QUESTION 1

- (Topic 1)

IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 2

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:

B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this area.

D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

#### NEW QUESTION 3

- (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 4

- (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 5

- (Topic 1)

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

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

**Answer:**

D

**Explanation:**

A completely connected mesh configuration creates a direct link between any two host machines.

**NEW QUESTION 6**

- (Topic 1)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 7**

- (Topic 1)

A database administrator is responsible for:

- A. defining data ownershi
- B. establishing operational standards for the data dictionar
- C. creating the logical and physical databas
- D. establishing ground rules for ensuring data integrity and securit

**Answer: C**

**Explanation:**

A database administrator is responsible for creating and controlling the logical and physical database. Defining data ownership resides with the head of the user department or top management if the data is common to the organization. IS management and the data administrator are responsible for establishing operational standards for the data dictionary. Establishing ground rules for ensuring data integrity and security in line with the corporate security policy is a function of the security administrator.

**NEW QUESTION 8**

- (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 9**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

#### NEW QUESTION 10

- (Topic 1)

A LAN administrator normally would be restricted from:

- A. having end-user responsibilitie
- B. reporting to the end-user manage
- C. having programming responsibilitie
- 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 is a telecommunication device that translates data from digital form to analog form and back to digital?

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 14

- (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 16

- (Topic 1)

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

- A. duplicate chec
- B. table looku
- C. validity chec
- D. parity chec

**Answer:** D

**Explanation:**

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

#### NEW QUESTION 20

- (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 21

- (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 24

- (Topic 1)

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

- A. Relocate the shut off switch
- B. Install protective cover
- C. Escort visitor
- D. Log environmental failure

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 28

- (Topic 1)

Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

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

**Answer: B**

#### Explanation:

A quality plan is an essential element of all projects. It is critical that the contracted supplier be required to produce such a plan. The quality plan for the proposed development contract should be comprehensive and encompass all phases of the development and include which business functions will be included and when. Acceptance is normally managed by the user area, since they must be satisfied that the new system will meet their requirements. If the system is large, a phased-in approach to implementing the application is a reasonable approach. Prototyping is a valid method of ensuring that the system will meet business requirements.

#### NEW QUESTION 32

- (Topic 1)

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

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

**Answer: A**

#### Explanation:

A RA is an entity that is responsible for identification and authentication of certificate subjects, but the RA does not sign or issue certificates. The certificate subject usually interacts with the RA for completing the process of subscribing to the services of the certification authority in terms of getting identity validated with standard identification documents, as detailed in the certificate policies of the CA. In the context of a particular certificate, the issuing CA is the CA that issued the certificate. In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate.

#### NEW QUESTION 36

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 38

- (Topic 1)

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

- A. reasonableness chec
- B. parity chec
- C. redundancy chec
- D. check digit

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 42

- (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 43

- (Topic 1)

What is the PRIMARY purpose of audit trails?

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 47

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 51

- (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 56**

- (Topic 1)

What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 58**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 59**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 63**

- (Topic 1)

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

- A. True
- B. False

**Answer:** B

**Explanation:**

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

**NEW QUESTION 68**

- (Topic 1)

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

- A. Detective
- B. Corrective
- C. Preventative
- D. Compensatory

**Answer:** D

**Explanation:**

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

**NEW QUESTION 72**

- (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 76**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 80**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 82**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 84**

- (Topic 1)

What increases encryption overhead and cost the most?

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 89**

- (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 92

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 95

- (Topic 1)

How does the SSL network protocol provide confidentiality?

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 98

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 103

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 108

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

Logical access controls are often the primary safeguards for systems software and data.

Which of the following is often used as a detection and deterrent control against Internet

attacks? A. Honeypots B. CCTV C. VPN D. VLAN Answer: A Honeypots are often used as a detection and deterrent control against Internet attacks.

#### NEW QUESTION 112

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

Biometrics can be used to provide excellent physical access control.

#### NEW QUESTION 115

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 116

- (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 119

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 120

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 122

- (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 126**

- (Topic 1)

Library control software restricts source code to:

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 128**

- (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 131**

- (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 134**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 135**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 137**

- (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 139**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 143**

- (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 147**

- (Topic 1)

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

- A. True
- B. False

**Answer:** A

**Explanation:**

Fourth-generation languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures.

**NEW QUESTION 148**

- (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 149**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 151**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 152**

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 155**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 160**

- (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 163**

- (Topic 1)

Parity bits are a control used to validate:

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

**Answer:** B

**Explanation:**

Parity bits are a control used to validate data completeness.

**NEW QUESTION 168**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 172**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 175**

- (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 177**

- (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 182**

- (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 186

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 187

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 190

- (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 191

- (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 195

- (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 200

- (Topic 1)

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

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 205**

- (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 207**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 208**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 213**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 214**

- (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 218

- (Topic 1)

What can be used to gather evidence of network attacks?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 219

- (Topic 1)

What is a callback system?

- A. It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fail
- B. It is a remote-access system whereby the user's application automatically redials the remoteaccess server if the initial connection attempt fail
- C. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration databas
- D. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of tim

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 223

- (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 227

- (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 231

- (Topic 1)

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

- A. True
- B. False

**Answer:** A

#### Explanation:

If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions.

#### NEW QUESTION 233

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 236

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 241

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

If a database is restored from information backed up before the last system image, the system should be restarted before the last transaction because the final transaction must be reprocessed.

#### NEW QUESTION 245

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 250

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 251

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 255**

- (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 260**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 263**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 267**

- (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 272**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 273**

- (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 276**

- (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 277**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 280**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

Transaction authorization is the primary security concern for EDI environments.

**NEW QUESTION 285**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**



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

#### NEW QUESTION 286

- (Topic 1)

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

- A. Deterrent integrity controls
- B. Detective integrity controls
- C. Corrective integrity controls
- D. Preventative integrity controls

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 287

- (Topic 1)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 292

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 297

- (Topic 2)

An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

- A. variable samplin
- B. substantive testin
- C. compliance testin
- D. stop-or-go samplin

**Answer:** C

#### Explanation:

Compliance testing determines whether controls are being applied in compliance with policy. This includes tests to determine whether new accounts were appropriately authorized. Variable sampling is used to estimate numerical values, such as dollar values. Substantive testing substantiates the integrity of actual processing, such as balances on financial statements. The development of substantive tests is often dependent on the outcome of compliance tests. If compliance tests indicate that there are adequate internal controls, then substantive tests can be minimized. Stop-or-go sampling allows a test to be stopped as early as possible and is not appropriate for checking whether procedures have been followed.

#### NEW QUESTION 299

- (Topic 2)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 300

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 305

- (Topic 2)

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

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

**Answer:** D

#### Explanation:

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various scheduling methods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

#### NEW QUESTION 309

- (Topic 2)

An audit charter should:

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 314

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 317

- (Topic 2)

The PRIMARY purpose of audit trails is to:

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

**Answer:**

B

**Explanation:**

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

**NEW QUESTION 322**

- (Topic 2)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 326**

- (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 327**

- (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 329**

- (Topic 2)

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

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

**Answer: D**

**Explanation:**

The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and the scope of the audit should not be limited by the auditee's ability to find relevant evidence.

#### NEW QUESTION 332

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 337

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 340

- (Topic 2)

The PRIMARY purpose of an IT forensic audit is:

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 341

- (Topic 2)

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

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

**Answer:** D

#### Explanation:

Audit standards require that an IS auditor gather sufficient and appropriate audit evidence. The auditor has found a potential problem and now needs to determine if this is an isolated incident or a systematic control failure. At this stage it is too preliminary to issue an audit finding and seeking an explanation from management is advisable, but it would be better to gather additional evidence to properly evaluate the seriousness of the situation. A backup failure, which has not been established at this point, will be serious if it involves critical data. However, the issue is not the importance of the data on the server, where a problem has been detected, but whether a systematic control failure that impacts other servers exists.

#### NEW QUESTION 342

- (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 344

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 346

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

Not reporting an intrusion is equivalent to an IS auditor hiding a malicious intrusion, which would be a professional mistake. Although notification to the police may be required and the lack of a periodic examination of access rights might be a concern, they do not represent as big a concern as the failure to report the attack. Reporting to the public is not a requirement and is dependent on the organization's desire, or lack thereof, to make the intrusion known.

#### NEW QUESTION 347

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 348

- (Topic 2)

Data flow diagrams are used by IS auditors to:

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

**Answer:** C

**Explanation:**

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and



storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

#### NEW QUESTION 353

- (Topic 2)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 358

- (Topic 2)

An IS auditor reviews an organizational chart PRIMARILY for:

- A. an understanding of workflow
- B. investigating various communication channel
- C. understanding the responsibilities and authority of individual
- D. investigating the network connected to different employee

**Answer:** C

#### Explanation:

An organizational chart provides information about the responsibilities and authority of individuals in the organization. This helps an IS auditor to know if there is a proper segregation of functions. A workflow chart would provide information about the roles of different employees. A network diagram will provide information about the usage of various communication channels and will indicate the connection of users to the network.

#### NEW QUESTION 362

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 367

- (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 370

- (Topic 2)

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

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



**Answer:** C

**Explanation:**

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

#### NEW QUESTION 375

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially-written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audit trail is required.

#### NEW QUESTION 378

- (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 381

- (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 process
- B. comply with auditing standard
- C. identify control weaknesses
- D. plan substantive testing

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 384

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 387

- (Topic 2)

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

- A. audit trail of the versioning of the work paper
- B. approval of the audit phase
- C. access rights to the work paper
- D. confidentiality of the work paper

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 391

- (Topic 2)

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

- A. comply with regulatory requirement
- B. provide a basis for drawing reasonable conclusion
- C. ensure complete audit coverag
- D. perform the audit according to the defined scop

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 394

- (Topic 2)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 395

- (Topic 2)

During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 396

- (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 softwar
- B. Inform the auditee of the unauthorized software, and follow up to confirm deletio
- C. Report the use of the unauthorized software and the need to prevent recurrence to auditee managemen
- D. Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such us

**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 398

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

ISACA's standard on 'reporting' requires the IS auditor have sufficient and appropriate audit evidence to support the reported results. Statements from IS management provide a basis for obtaining concurrence on matters that cannot be verified with empirical evidence. The report should be based on evidence collected during the course of the review even though the auditor may have access to the work papers of other auditors. The results of an organizational control self-assessment (CSA) could supplement the audit findings. Choices A, B and C might be referenced during an audit but, of themselves, would not be considered a sufficient basis for issuing a report.

#### NEW QUESTION 400

- (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 403

- (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, control
- C. the implementation of a stringent control policy and rule-driven control
- 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 407

- (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 411

- (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 416

- (Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 421

- (Topic 3)

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

- A. strategic plan
- B. IS policies
- C. IS procedure
- D. standards and guideline

**Answer:** A

#### Explanation:

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

#### NEW QUESTION 425

- (Topic 3)

Establishing the level of acceptable risk is the responsibility of:

- A. quality assurance management
- B. senior business management
- C. the chief information office
- D. the chief security office

**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 430

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

- A. chief executive office
- B. board of director
- C. IT steering committee
- D. audit committee

**Answer:** B

**Explanation:**

IT governance is primarily the responsibility of the executives and shareholders (as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

**NEW QUESTION 434**

- (Topic 3)

As an outcome of information security governance, strategic alignment provides:

- A. security requirements driven by enterprise requirement
- B. baseline security following best practice
- C. institutionalized and commoditized solution
- D. an understanding of risk exposure

**Answer:** A

**Explanation:**

Information security governance, when properly implemented, should provide four basic outcomes: strategic alignment, value delivery, risk management and performance measurement. Strategic alignment provides input for security requirements driven by enterprise requirements. Value delivery provides a standard set of security practices, i.e., baseline security following best practices or institutionalized and commoditized solutions. Risk management provides an understanding of risk exposure.

**NEW QUESTION 439**

- (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 440**

- (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 444**

- (Topic 3)

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

- A. provide instructions on how to do the job and define authority
- B. are current, documented and readily available to the employee
- C. communicate management's specific job performance expectation
- D. establish responsibility and accountability for the employee's action

**Answer:** D

**Explanation:**

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

**NEW QUESTION 449**

- (Topic 3)



Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

- A. ensure the employee maintains a good quality of life, which will lead to greater productivity
- B. reduce the opportunity for an employee to commit an improper or illegal act
- C. provide proper cross-training for another employee
- D. eliminate the potential disruption caused when an employee takes vacation one day at a time

**Answer: B**

**Explanation:**

Required vacations/holidays of a week or more in duration in which someone other than the regular employee performs the job function is often mandatory for sensitive positions, as this reduces the opportunity to commit improper or illegal acts. During this time it may be possible to discover any fraudulent activity that was taking place. Choices A, C and D could all be organizational benefits from a mandatory vacation policy, but they are not the reason why the policy is established.

#### NEW QUESTION 454

- (Topic 3)

A local area network (LAN) administrator normally would be restricted from:

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

**Answer: C**

**Explanation:**

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

#### NEW QUESTION 455

- (Topic 3)

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

- A. length of service, since this will help ensure technical competency
- B. age, as training in audit techniques may be impractical
- C. IS knowledge, since this will bring enhanced credibility to the audit function
- D. ability, as an IS auditor, to be independent of existing IS relationship

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 460

- (Topic 3)

When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

- A. Restricting physical access to computing equipment
- B. Reviewing transaction and application logs
- C. Performing background checks prior to hiring IT staff
- D. Locking user sessions after a specified period of inactivity

**Answer: B**

**Explanation:**

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure IT staff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently) of access privileges that have officially been granted.

#### NEW QUESTION 464

- (Topic 3)

An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

- A. dependency on a single person
- B. inadequate succession planning



- C. one person knowing all parts of a system
- D. a disruption of operation

**Answer:** C

**Explanation:**

Cross-training is a process of training more than one individual to perform a specific job or procedure. This practice helps decrease the dependence on a single person and assists in succession planning. This provides for the backup of personnel in the event of an absence and, thereby, provides for the continuity of operations. However, in using this approach, it is prudent to have first assessed the risk of any person knowing all parts of a system and the related potential exposures. Cross-training reduces the risks addressed in choices A, B and D.

#### NEW QUESTION 469

- (Topic 3)

Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

- A. Overlapping controls
- B. Boundary controls
- C. Access controls
- D. Compensating controls

**Answer:** D

**Explanation:**

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

#### NEW QUESTION 470

- (Topic 3)

Which of the following reduces the potential impact of social engineering attacks?

- A. Compliance with regulatory requirements
- B. Promoting ethical understanding
- C. Security awareness programs
- D. Effective performance incentives

**Answer:** C

**Explanation:**

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

#### NEW QUESTION 474

- (Topic 3)

Which of the following is a risk of cross-training?

- A. Increases the dependence on one employee
- B. Does not assist in succession planning
- C. One employee may know all parts of a system
- D. Does not help in achieving a continuity of operations

**Answer:** C

**Explanation:**

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

#### NEW QUESTION 477

- (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 482

- (Topic 3)

To support an organization's goals, an IS department should have:

- A. a low-cost philosoph
- B. long- and short-range plan
- C. leading-edge technolog
- D. plans to acquire new hardware and softwar

**Answer:** B

#### Explanation:

To ensure its contribution to the realization of an organization's overall goals, the IS department should have long- and short-range plans that are consistent with the organization's broader plans for attaining its goals. Choices A and C are objectives, and plans would be needed to delineate how each of the objectives would be achieved. Choice D could be a part of the overall plan but would be required only if hardware or software is needed to achieve the organizational goals.

#### NEW QUESTION 487

- (Topic 3)

In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

- A. there is an integration of IS and business staffs within project
- B. there is a clear definition of the IS mission and visio
- C. a strategic information technology planning methodology is in plac
- D. the plan correlates business objectives to IS goals and objective

**Answer:** A

#### Explanation:

The integration of IS and business staff in projects is an operational issue and should be considered while reviewing the short-range plan. A strategic plan would provide a framework for the IS short-range plan. Choices B, C and D are areas covered by a strategic plan.

#### NEW QUESTION 489

- (Topic 3)

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

- A. Test a new accounting packag
- B. Perform an evaluation of information technology need
- C. Implement a new project planning system within the next 12 month
- D. Become the supplier of choice for the product offere

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 493

- (Topic 3)

Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

- A. has been approved by line managemen
- B. does not vary from the IS department's preliminary budge
- C. complies with procurement procedure
- D. supports the business objectives of the organizatio

**Answer:** D

#### Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrect since line management prepared the plans.

#### NEW QUESTION 498

- (Topic 3)

An IS auditor reviewing an organization's IT strategic plan should FIRST review:

- A. the existing IT environmen
- B. the business pla

- C. the present IT budge
- D. current technology trend

**Answer:** B

**Explanation:**

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

#### NEW QUESTION 501

- (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 effective
- 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 505

- (Topic 3)

The rate of change in technology increases the importance of:

- A. outsourcing the IS functio
- B. implementing and enforcing good processe
- C. hiring personnel willing to make a career within the organizatio
- D. meeting user requirement

**Answer:** B

**Explanation:**

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

#### NEW QUESTION 510

- (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 511

- (Topic 3)

The development of an IS security policy is ultimately the responsibility of the:

- A. IS departmen
- B. security committe
- C. security administrato
- D. board of director

**Answer:** D

**Explanation:**

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

#### NEW QUESTION 516

- (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 520

- (Topic 3)

Which of the following is the initial step in creating a firewall policy?

- A. A cost-benefit analysis of methods for securing the applications
- B. Identification of network applications to be externally accessed
- C. Identification of vulnerabilities associated with network applications to be externally accessed
- D. Creation of an applications traffic matrix showing protection methods

**Answer: B**

#### Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

#### NEW QUESTION 521

- (Topic 3)

The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- A. Utilization of an intrusion detection system to report incidents
- B. Mandating the use of passwords to access all software
- C. Installing an efficient user log system to track the actions of each user
- D. Training provided on a regular basis to all current and new employees

**Answer: D**

#### Explanation:

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

#### NEW QUESTION 525

- (Topic 3)

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- A. Assimilation of the framework and intent of a written security policy by all appropriate parties
- B. Management support and approval for the implementation and maintenance of a security policy
- C. Enforcement of security rules by providing punitive actions for any violation of security rules
- D. Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

**Answer: A**

#### Explanation:

Assimilation of the framework and intent of a written security policy by the users of the system is critical to the successful implementation and maintenance of the security policy. A good password system may exist, but if the users of the system keep passwords written on their desk, the password is of little value. Management support and commitment is no doubt important, but for successful implementation and maintenance of security policy, educating the users on the importance of security is paramount. The stringent implementation, monitoring and enforcing of rules by the security officer through access control software, and provision for punitive actions for violation of security rules, is also required, along with the user's education on the importance of security.

#### NEW QUESTION 527

- (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 530

- (Topic 3)

A top-down approach to the development of operational policies will help ensure:

- A. that they are consistent across the organization
- B. that they are implemented as a part of risk assessment
- C. compliance with all policies
- D. that they are reviewed periodically

**Answer:** A

**Explanation:**

Deriving lower level policies from corporate policies (a top-down approach) aids in ensuring consistency across the organization and consistency with other policies. The bottom-up approach to the development of operational policies is derived as a result of risk assessment. A top-down approach of itself does not ensure compliance and development does not ensure that policies are reviewed.

#### NEW QUESTION 531

- (Topic 3)

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

- A. Time zone differences could impede communications between IT team
- B. Telecommunications cost could be much higher in the first year
- C. Privacy laws could prevent cross-border flow of information
- D. Software development may require more detailed specification

**Answer:** C

**Explanation:**

Privacy laws prohibiting the cross-border flow of personally identifiable information would make it impossible to locate a data warehouse containing customer information in another country. Time zone differences and higher telecommunications costs are more manageable. Software development typically requires more detailed specifications when dealing with offshore operations.

#### NEW QUESTION 534

- (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 537

- (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 542

- (Topic 3)

Which of the following provides the best evidence of the adequacy of a security awareness program?

- A. The number of stakeholders including employees trained at various levels
- B. Coverage of training at all locations across the enterprise
- C. The implementation of security devices from different vendors
- D. Periodic reviews and comparison with best practices

**Answer:** D

#### Explanation:

The adequacy of security awareness content can best be assessed by determining whether it is periodically reviewed and compared to industry best practices. Choices A, B and C provide metrics for measuring various aspects of a security awareness program, but do not help assess the content.

#### NEW QUESTION 547

- (Topic 3)

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

- A. provide strategic directio
- B. control business operation
- C. align IT with busines
- D. implement best practice

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 551

- (Topic 3)

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- A. Define a balanced scorecard (BSC) for measuring performance
- B. Consider user satisfaction in the key performance indicators (KPIs)
- C. Select projects according to business benefits and risks
- D. Modify the yearly process of defining the project portfolio

**Answer:** C

#### Explanation:

Prioritization of projects on the basis of their expected benefit(s) to business, and the related risks, is the best measure for achieving alignment of the project portfolio to an organization's strategic priorities. Modifying the yearly process of the projects portfolio definition might improve the situation, but only if the portfolio definition process is currently not tied to the definition of corporate strategies; however, this is unlikely since the difficulties are in maintaining the alignment, and not in setting it up initially. Measures such as balanced scorecard (BSC) and key performance indicators (KPIs) are helpful, but they do not guarantee that the projects are aligned with business strategy.

#### NEW QUESTION 553

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISA Product From:

<https://www.2passeasy.com/dumps/CISA/>

## Money Back Guarantee

### CISA Practice Exam Features:

- \* CISA Questions and Answers Updated Frequently
- \* CISA Practice Questions Verified by Expert Senior Certified Staff
- \* CISA Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year