



**Isaca**

## Exam Questions CISA

Isaca CISA

#### NEW QUESTION 1

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 2

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

A blackbox test is a dynamic analysis tool for testing software modules. During the testing of software modules a blackbox test works first in a cohesive manner as one single unit/entity, consisting of numerous modules and second, with the user data that flows across software modules. In some cases, this even drives the software behavior.

#### NEW QUESTION 3

- (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 4

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 5

- (Topic 1)

The use of a GANTT chart can:

- A. aid in scheduling project task
- B. determine project checkpoint
- C. ensure documentation standard
- D. direct the post-implementation revie

**Answer:** A

**Explanation:**

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

**NEW QUESTION 6**

- (Topic 1)

A hub is a device that connects:

- A. two LANs using different protocol
- B. a LAN with a WA
- C. a LAN with a metropolitan area network (MAN).
- D. two segments of a single LA

**Answer:** D

**Explanation:**

A hub is a device that connects two segments of a single LAN. A hub is a repeater. It provides transparent connectivity to users on all segments of the same LAN. It is a level 1 device.

**NEW QUESTION 7**

- (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 8**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 9**

- (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 10**

- (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 authorit

**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 10

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 15

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 18

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 22

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 27

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 29**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 33**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 34**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

Electronic data interface (EDI) supports intervendor communication while decreasing the time necessary for review because it is usually configured to readily identify errors requiring follow-up.

**NEW QUESTION 38**

- (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 39**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 42

- (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 44

- (Topic 1)

Which of the following best characterizes "worms"?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 49

- (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 50

- (Topic 1)

Which of the following do digital signatures provide?

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

**Answer:** A

#### Explanation:

The primary purpose of digital signatures is to provide authentication and integrity of data.

#### NEW QUESTION 54

- (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 57

- (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 62**

- (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 67**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 70**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 71**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 72**

- (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 75**

- (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 80**

- (Topic 1)

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

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

**Answer: B**

**Explanation:**

Run-to-run totals can verify data through various stages of application processing.

**NEW QUESTION 81**

- (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 82**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

Data-mining techniques can be used to help identify and investigate unauthorized transactions.

**NEW QUESTION 83**

- (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 88**

- (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 93**

- (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 96**

- (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 100**

- (Topic 1)

Why does an IS auditor review an organization chart?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 104**

- (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 109**

- (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 110

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

#### NEW QUESTION 115

- (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 119

- (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 122

- (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 127

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 131

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 134**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 139**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

A website certificate is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption.

**NEW QUESTION 140**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 144**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 147**

- (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 152**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 154**

- (Topic 1)

Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 159**

- (Topic 1)

Off-site data backup and storage should be geographically separated so as to \_\_\_\_\_ (fill in the blank) the risk of a widespread physical disaster such as a hurricane or earthquake.

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

**Answer:** D

**Explanation:**

Off-site data backup and storage should be geographically separated, to mitigate the risk of a widespread physical disaster such as a hurricane or an earthquake.

**NEW QUESTION 161**

- (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 165**

- (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 169**

- (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 171**

- (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 172**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 177**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 178**

- (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 180**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 185**

- (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 188**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 189**

- (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 194**

- (Topic 2)

An audit charter should:

- A. be dynamic and change often to coincide with the changing nature of technology and the audit professio
- 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 functio

**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 198**

- (Topic 2)

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

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

**Answer: A**

**Explanation:**

Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for



the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

#### NEW QUESTION 203

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples. Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

#### NEW QUESTION 204

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 206

- (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 207

- (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 210

- (Topic 2)

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



- A. efficiency of the application in meeting the business processe
- B. impact of any exposures discovere
- C. business processes served by the applicatio
- D. application's optimizatio

**Answer:** B

**Explanation:**

An application control review involves the evaluation of the application's automated controls and an assessment of any exposures resulting from the control weaknesses. The other choices may be objectives of an application audit but are not part of an audit restricted to a review of controls.

#### NEW QUESTION 213

- (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 mechanis
- B. Clear the virus from the networ
- C. Inform appropriate personnel immediatel
- D. Ensure deletion of the viru

**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 217

- (Topic 2)

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

- A. analysi
- B. evaluatio
- C. preservatio
- D. disclosur

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 220

- (Topic 2)

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

- A. professional independence
- B. organizational independenc
- C. technical competenc
- D. professional competenc

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 225

- (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 228

- (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 coverage
- D. perform the audit according to the defined scope

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 230

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 233

- (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 235

- (Topic 2)

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

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

**Answer: C**

#### Explanation:

The use of unauthorized or illegal software should be prohibited by an organization. Software piracy results in inherent exposure and can result in severe fines. An IS auditor must convince the user and user management of the risk and the need to eliminate the risk. An IS auditor should not assume the role of the enforcing officer and take on any personal involvement in removing or deleting the unauthorized software.

#### NEW QUESTION 237

- (Topic 2)

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

- A. having line managers assume a portion of the responsibility for control monitorin
- 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 dutie

**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 242

- (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 adequat
- C. the stability of existing softwar
- D. the complexity of installed technolog

**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 247

- (Topic 3)

An IS steering committee should:

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 250

- (Topic 3)

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

- A. IT budge
- B. existing IT environmen
- C. business pla
- D. investment pla

**Answer:** C

**Explanation:**

One of the most important reasons for which projects get funded is how well a project meets an organization's strategic objectives. Portfolio management takes a holistic view of a company's overall IT strategy. IT strategy should be aligned with the business strategy and, hence, reviewing the business plan should be the major consideration. Choices A, B and D are important but secondary to the importance of reviewing the business plan.

#### NEW QUESTION 254

- (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 256

- (Topic 3)

Which of the following would BEST provide assurance of the integrity of new staff?

- A. Background screening
- B. References
- C. Bonding
- D. Qualifications listed on a resume

**Answer:** A

#### Explanation:

A background screening is the primary method for assuring the integrity of a prospective staff member. References are important and would need to be verified, but they are not as reliable as background screening. Bonding is directed at due-diligence compliance, not at integrity, and qualifications listed on a resume may not be accurate.

#### NEW QUESTION 261

- (Topic 3)

When an employee is terminated from service, the MOST important action is to:

- A. hand over all of the employee's files to another designated employee
- B. complete a backup of the employee's work
- C. notify other employees of the termination
- D. disable the employee's logical access

**Answer:** D

#### Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

#### NEW QUESTION 264

- (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 266

- (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 269

- (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 270

- (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 273

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 277

- (Topic 3)

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

- A. a low-cost philosophy
- B. long- and short-range plans
- C. leading-edge technology
- D. plans to acquire new hardware and software

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 279

- (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 vision
- C. a strategic information technology planning methodology is in place
- D. the plan correlates business objectives to IS goals and objectives

**Answer:** A

**Explanation:**



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

#### NEW QUESTION 284

- (Topic 3)

Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

- A. Allocating resources
- B. Keeping current with technology advances
- C. Conducting control self-assessment
- D. Evaluating hardware needs

**Answer:** A

#### Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

#### NEW QUESTION 287

- (Topic 3)

When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

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

**Answer:** B

#### Explanation:

Determining if the IS plan is consistent with management strategy relates IS/IT planning to business plans. Choices A, C and D are effective methods for determining the alignment of IS plans with business objectives and the organization's strategies.

#### NEW QUESTION 291

- (Topic 3)

To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

- A. control self-assessment
- B. a business impact analysi
- C. an IT balanced scorecar
- D. business process reengineerin

**Answer:** C

#### Explanation:

An IT balanced scorecard (BSC) provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. Control self-assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

#### NEW QUESTION 294

- (Topic 3)

When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

- A. establishment of a review boar
- B. creation of a security uni
- C. effective support of an executive sponso
- D. selection of a security process owne

**Answer:** C

#### Explanation:

The executive sponsor would be in charge of supporting the organization's strategic security program, and would aid in directing the organization's overall security management activities. Therefore, support by the executive level of management is the most critical success factor (CSF). None of the other choices are effective without visible sponsorship of top management.

#### NEW QUESTION 299

- (Topic 3)

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- A. an assessment of the fit of the organization's application portfolio with business objective
- B. actions to reduce hardware procurement cos

- C. a listing of approved suppliers of IT contract resource
- D. a description of the technical architecture for the organization's network perimeter security

**Answer:** A

**Explanation:**

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is to set out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail of a specific technical architecture.

**NEW QUESTION 300**

- (Topic 3)

The rate of change in technology increases the importance of:

- A. outsourcing the IS function
- B. implementing and enforcing good processes
- C. hiring personnel willing to make a career within the organization
- D. meeting user requirements

**Answer:** B

**Explanation:**

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

**NEW QUESTION 301**

- (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 306**

- (Topic 3)

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- A. implementation
- B. compliance
- C. documentation
- D. sufficiency

**Answer:** D

**Explanation:**

An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

**NEW QUESTION 307**

- (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 308

- (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 312

- (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 314

- (Topic 3)

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

- A. project management tool
- B. an object-oriented architecture
- C. tactical planning
- D. enterprise architecture (EA).

**Answer: D**

#### Explanation:

Enterprise architecture (EA) involves documenting the organization's IT assets and processes in a structured manner to facilitate understanding, management and planning for IT investments. It involves both a current state and a representation of an optimized future state. In attempting to complete an EA, organizations can address the problem either from a technology perspective or a business process perspective. Project management does not consider IT investment aspects; it is a tool to aid in delivering projects. Object-oriented architecture is a software development methodology and does not assist in planning for IT investment, while tactical planning is relevant only after high-level IT investment decisions have been made.

#### NEW QUESTION 315

- (Topic 3)

A benefit of open system architecture is that it:

- A. facilitates interoperability
- B. facilitates the integration of proprietary component
- C. will be a basis for volume discounts from equipment vendor
- D. allows for the achievement of more economies of scale for equipment

**Answer: A**

#### Explanation:

Open systems are those for which suppliers provide components whose interfaces are defined by public standards, thus facilitating interoperability between systems made by different vendors. In contrast, closed system components are built to proprietary standards so that other suppliers' systems cannot or will not interface with existing systems.

#### NEW QUESTION 316

- (Topic 3)

After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

- A. Project management and progress reporting is combined in a project management office which is driven by external consultant
- B. The replacement effort consists of several independent projects without integrating the resource allocation in a portfolio management approach
- C. The resources of each of the organizations are inefficiently allocated while they are being familiarized with the other company's legacy system
- D. The new platform will force the business areas of both organizations to change their work processes, which will result in extensive training need

**Answer:** B

**Explanation:**

The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralized dependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. It is a good idea to first get familiar with the old systems, to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs as organizations and processes change to leverage the intended synergy effects of the merger.

#### NEW QUESTION 318

- (Topic 3)

With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

- A. Outsourced activities are core and provide a differentiated advantage to the organization
- B. Periodic renegotiation is specified in the outsourcing contract
- C. The outsourcing contract fails to cover every action required by the arrangement
- D. Similar activities are outsourced to more than one vendor

**Answer:** A

**Explanation:**

An organization's core activities generally should not be outsourced, because they are what the organization does best; an IS auditor observing that should be concerned. An IS auditor should not be concerned about the other conditions because specification of periodic renegotiation in the outsourcing contract is a best practice. Outsourcing contracts cannot be expected to cover every action and detail expected of the parties involved, while multisourcing is an acceptable way to reduce risk.

#### NEW QUESTION 321

- (Topic 3)

An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

- A. Report the risks to the CIO and CEO immediately
- B. Examine e-business application in development
- C. Identify threats and likelihood of occurrence
- D. Check the budget available for risk management

**Answer:** C

**Explanation:**

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

#### NEW QUESTION 323

- (Topic 3)

When developing a risk management program, what is the FIRST activity to be performed?

- A. Threat assessment
- B. Classification of data
- C. Inventory of assets
- D. Criticality analysis

**Answer:** C

**Explanation:**

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

#### NEW QUESTION 324

- (Topic 3)

A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

- A. compute the amortization of the related asset
- B. calculate a return on investment (ROI).
- C. apply a qualitative approach
- D. spend the time needed to define exactly the loss amount

**Answer:** C

**Explanation:**

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor {e.g., one is a very low impact to the business and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

**NEW QUESTION 328**

- (Topic 3)

Assessing IT risks is BEST achieved by:

- A. evaluating threats associated with existing IT assets and IT project
- B. using the firm's past actual loss experience to determine current exposure
- C. reviewing published loss statistics from comparable organization
- D. reviewing IT control weaknesses identified in audit report

**Answer: A**

**Explanation:**

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient. Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to be assessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

**NEW QUESTION 332**

- (Topic 3)

To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

- A. avoidance
- B. transference
- C. mitigation
- D. acceptance

**Answer: C**

**Explanation:**

Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage. Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

**NEW QUESTION 333**

- (Topic 3)

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

- A. vulnerabilities
- B. threat
- C. probabilities
- D. impact

**Answer: A**

**Explanation:**

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

**NEW QUESTION 338**

- (Topic 3)

Which of the following should be considered FIRST when implementing a risk management program?

- A. An understanding of the organization's threat, vulnerability and risk profile
- B. An understanding of the risk exposures and the potential consequences of compromise
- C. A determination of risk management priorities based on potential consequences
- D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

**Answer: A**

**Explanation:**

Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's

threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

#### NEW QUESTION 340

- (Topic 3)

As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

- A. performance measuremen
- B. strategic alignmen
- C. value deliver
- D. resource managemen

**Answer:** A

#### Explanation:

Performance measurement includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how they deliver it (process capability and performance). Strategic alignment primarily focuses on ensuring linkage of business and IT plans. Value delivery is about executing the value proposition throughout the delivery cycle. Resource management is about the optimal investment in and proper management of critical IT resources. Transparency is primarily achieved through performance measurement as it provides information to the stakeholders on how well the enterprise is performing when compared to objectives.

#### NEW QUESTION 344

- (Topic 3)

Which of the following is the PRIMARY objective of an IT performance measurement process?

- A. Minimize errors
- B. Gather performance data
- C. Establish performance baselines
- D. Optimize performance

**Answer:** D

#### Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

#### NEW QUESTION 348

- (Topic 4)

When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

- A. a clear business case has been approved by managemen
- B. corporate security standards will be me
- C. users will be involved in the implementation pla
- D. the new system will meet all required user functionalit

**Answer:** A

#### Explanation:

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs of the users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditor's first concern.

#### NEW QUESTION 350

- (Topic 4)

Which of the following risks could result from inadequate software baselining?

- A. Scope creep
- B. Sign-off delays
- C. Software integrity violations
- D. inadequate controls

**Answer:** A

#### Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a business cost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. Choices B, C and D may not always result, but choice A is inevitable.

#### NEW QUESTION 355

- (Topic 4)

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no

longer valid. The IS auditor should recommend that the:

- A. project be discontinued
- B. business case be updated and possible corrective actions be identified
- C. project be returned to the project sponsor for reapproval
- D. project be completed and the business case be updated late

**Answer: B**

**Explanation:**

An IS auditor should not recommend discontinuing or completing the project before reviewing an updated business case. The IS auditor should recommend that the business case be kept current throughout the project since it is a key input to decisions made throughout the life of any project.

#### NEW QUESTION 359

- (Topic 4)

The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

- A. integrity
- B. authenticity
- C. authorization
- D. nonrepudiation

**Answer: A**

**Explanation:**

A checksum calculated on an amount field and included in the EDI communication can be used to identify unauthorized modifications. Authenticity and authorization cannot be established by a checksum alone and need other controls. Nonrepudiation can be ensured by using digital signatures.

#### NEW QUESTION 364

- (Topic 4)

Which of the following will BEST ensure the successful offshore development of business applications?

- A. Stringent contract management practices
- B. Detailed and correctly applied specifications
- C. Awareness of cultural and political differences
- D. Postimplementation reviews

**Answer: B**

**Explanation:**

When dealing with offshore operations, it is essential that detailed specifications be created. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptions and modifications may not be adequately communicated. Contract management practices, cultural and political differences, and postimplementation reviews, although important, are not as pivotal to the success of the project.

#### NEW QUESTION 367

- (Topic 4)

An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

- A. continuous improvement
- B. quantitative quality goal
- C. a documented process
- D. a process tailored to specific project

**Answer: A**

**Explanation:**

An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

#### NEW QUESTION 369

- (Topic 4)

Which of the following is the most important element in the design of a data warehouse?

- A. Quality of the metadata
- B. Speed of the transactions
- C. Volatility of the data
- D. Vulnerability of the system

**Answer: A**

**Explanation:**

Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for



query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

#### NEW QUESTION 372

- (Topic 4)

Ideally, stress testing should be carried out in a:

- A. test environment using test data
- B. production environment using live workload
- C. test environment using live workload
- D. production environment using test data

**Answer: C**

#### Explanation:

Stress testing is carried out to ensure a system can cope with production workloads. A test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment (choices B and D), and if only test data is used, there is no certainty that the system was stress tested adequately.

#### NEW QUESTION 374

- (Topic 4)

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

- A. Black box test
- B. Desk checking
- C. Structured walkthrough
- D. Design and code

**Answer: A**

#### Explanation:

A black box test is a dynamic analysis tool for testing software modules. During the testing of software modules a black box test works first in a cohesive manner as a single unit/entity consisting of numerous modules, and second with the user data that flows across software modules, in some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

#### NEW QUESTION 379

- (Topic 4)

A decision support system (DSS):

- A. is aimed at solving highly structured problem
- B. combines the use of models with nontraditional data access and retrieval function
- C. emphasizes flexibility in the decision making approach of user
- D. supports only structured decision making task

**Answer: C**

#### Explanation:

DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semistructured decision making tasks.

#### NEW QUESTION 381

- (Topic 4)

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

- A. interface errors are detected earlier
- B. confidence in the system is achieved earlier
- C. errors in critical modules are detected earlier
- D. major functions and processing are tested earlier

**Answer: C**

#### Explanation:

The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and works upward until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices in this question all refer to advantages of a top-down approach, which follows the opposite path, either in depth-first or breadth-first search order.

#### NEW QUESTION 382

- (Topic 4)

When a new system is to be implemented within a short time frame, it is MOST important to:

- A. finish writing user manual
- B. perform user acceptance testing

- C. add last-minute enhancements to functionalitie
- D. ensure that the code has been documented and reviewe

**Answer:** B

**Explanation:**

It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirements.

#### NEW QUESTION 387

- (Topic 4)

An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

- A. a backup server be available to run ETCS operations with up-to-date dat
- B. a backup server be loaded with all the relevant software and dat
- C. the systems staff of the organization be trained to handle any even
- D. source code of the ETCS application be placed in escro

**Answer:** D

**Explanation:**

Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business. Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

#### NEW QUESTION 390

- (Topic 4)

Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

- A. Intrusion detection systems
- B. Data mining techniques
- C. Firewalls
- D. Packet filtering routers

**Answer:** B

**Explanation:**

Data mining is a technique used to detect trends or patterns of transactions or data. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

#### NEW QUESTION 393

- (Topic 4)

During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

- A. increased maintenanc
- B. improper documentation of testin
- C. inadequate functional testin
- D. delays in problem resolutio

**Answer:** C

**Explanation:**

The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B and D are not as important.

#### NEW QUESTION 396

- (Topic 4)

The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

- A. facilitates user involvemen
- B. allows early testing of technical feature
- C. facilitates conversion to the new syste
- D. shortens the development time fram

**Answer:** D

**Explanation:**

The greatest advantage of RAD is the shorter time frame for the development of a system. Choices A and B are true, but they are also true for the traditional



systems development life cycle. Choice C is not necessarily always true.

#### NEW QUESTION 401

- (Topic 4)

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

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

**Answer:** C

#### Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. A conceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

#### NEW QUESTION 405

- (Topic 4)

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- A. System owners
- B. System users
- C. System designers
- D. System builders

**Answer:** A

#### Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system. Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

#### NEW QUESTION 407

- (Topic 4)

The MAJOR advantage of a component-based development approach is the:

- A. ability to manage an unrestricted variety of data type
- B. provision for modeling complex relationship
- C. capacity to meet the demands of a changing environment
- D. support of multiple development environment

**Answer:** D

#### Explanation:

Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not the most significant advantages of a component-based development approach.

#### NEW QUESTION 411

- (Topic 4)

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

- A. Direct cutover
- B. Pilot study
- C. Phased approach
- D. Parallel run

**Answer:** D

#### Explanation:

Parallel runs are the safest-though the most expensive-approach, because both the old and new systems are run, thus incurring what might appear to be double costs. Direct cutover is actually quite risky, since it does not provide for a 'shake down period' nor does it provide an easy fallback option. Both a pilot study and a phased approach are performed incrementally, making rollback procedures difficult to execute.

#### NEW QUESTION 415

- (Topic 4)

From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

- A. a big bang deployment after proof of concept

- B. prototyping and a one-phase deployment
- C. a deployment plan based on sequenced phase
- D. to simulate the new infrastructure before deployment

**Answer:** C

**Explanation:**

When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

#### NEW QUESTION 419

- (Topic 4)

The reason a certification and accreditation process is performed on critical systems is to ensure that:

- A. security compliance has been technically evaluated
- B. data have been encrypted and are ready to be stored
- C. the systems have been tested to run on different platforms
- D. the systems have followed the phases of a waterfall model

**Answer:** A

**Explanation:**

Certified and accredited systems are systems that have had their security compliance technically evaluated for running on a specific production server. Choice B is incorrect because not all data of certified systems are encrypted. Choice C is incorrect because certified systems are evaluated to run in a specific environment. A waterfall model is a software development methodology and not a reason for performing a certification and accrediting process.

#### NEW QUESTION 424

- (Topic 4)

During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

- A. implement data backup and recovery procedure
- B. Define standards and closely monitor for compliance
- C. Ensure that only authorized personnel can update the databases
- D. Establish controls to handle concurrent access problems

**Answer:** A

**Explanation:**

Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, while monitoring for compliance is a detective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

#### NEW QUESTION 429

- (Topic 4)

Responsibility and reporting lines cannot always be established when auditing automated systems since:

- A. diversified control makes ownership irrelevant
- B. staff traditionally changes jobs with greater frequency
- C. ownership is difficult to establish where resources are shared
- D. duties change frequently in the rapid development of technology

**Answer:** C

**Explanation:**

Because of the diversified nature of both data and application systems, the actual owner of data and applications may be hard to establish.

#### NEW QUESTION 432

- (Topic 4)

A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is MOST effective in providing reasonable assurance that the change was authorized?

- A. The system will not process the change until the clerk's manager confirms the change by entering an approval code
- B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager
- C. The system requires the clerk to enter an approval code
- D. The system displays a warning message to the clerk

**Answer:** A

**Explanation:**

Choice A would prevent or detect the use of an unauthorized interest rate. Choice B informs the manager after the fact that a change was made, thereby making it possible for transactions to use an unauthorized rate prior to management review. Choices C and D do not prevent the clerk from entering an unauthorized rate change.

#### NEW QUESTION 437

- (Topic 4)

When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

- A. excessive transaction turnaround time
- B. application interface failure
- C. improper transaction authorization
- D. nonvalidated batch total

**Answer: C**

#### Explanation:

Foremost among the risks associated with electronic data interchange (EDI) is improper transaction authorization. Since the interaction with the parties is electronic, there is no inherent authentication. The other choices, although risks, are not significant.

#### NEW QUESTION 440

- (Topic 4)

An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

- A. reverse engineering
- B. prototyping
- C. software reuse
- D. reengineering

**Answer: D**

#### Explanation:

Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

#### NEW QUESTION 442

- (Topic 4)

A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not performing adequately which of the following types of testing?

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

**Answer: B**

#### Explanation:

A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight). Units are tested by the programmer and then transferred to the acceptance test area; this often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

#### NEW QUESTION 446

- (Topic 4)

When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?

- A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks
- B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system
- C. A single implementation is planned, immediately decommissioning the legacy system
- D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software

**Answer: C**

#### Explanation:

Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy, should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

#### NEW QUESTION 449

- (Topic 5)

The PRIMARY objective of service-level management (SLM) is to:

- A. define, agree, record and manage the required levels of service
- B. ensure that services are managed to deliver the highest achievable level of availability
- C. keep the costs associated with any service at a minimum
- D. monitor and report any legal noncompliance to business management

**Answer:** A

**Explanation:**

The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services. This does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb. SLM cannot ensure that costs for all services will be kept at a low or minimum level, since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

#### NEW QUESTION 453

- (Topic 5)

Applying a retention date on a file will ensure that:

- A. data cannot be read until the date is set
- B. data will not be deleted before that date
- C. backup copies are not retained after that date
- D. datasets having the same name are differentiated

**Answer:** B

**Explanation:**

A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

#### NEW QUESTION 455

- (Topic 5)

The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:

- A. contents are highly volatile
- B. data cannot be backed up
- C. data can be copied
- D. device may not be compatible with other peripheral

**Answer:** C

**Explanation:**

Unless properly controlled, flash memory provides an avenue for anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

#### NEW QUESTION 459

- (Topic 5)

The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

- A. loss of confidentiality
- B. increased redundancy
- C. unauthorized accesses
- D. application malfunction

**Answer:** B

**Explanation:**

Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional and otherwise unnecessary data handling efforts. Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

#### NEW QUESTION 463

- (Topic 5)

Which of the following BEST limits the impact of server failures in a distributed environment?

- A. Redundant pathways
- B. Clustering
- C. Dial backup lines
- D. Standby power

**Answer:** B

**Explanation:**

Clustering allows two or more servers to work as a unit, so that when one of them fails, the other takes over. Choices A and C are intended to minimize the impact of channel communications failures, but not a server failure. Choice D provides an alternative power source in the event of an energy failure.

#### NEW QUESTION 468

- (Topic 5)

Doing which of the following during peak production hours could result in unexpected downtime?

- A. Performing data migration or tape backup
- B. Performing preventive maintenance on electrical systems
- C. Promoting applications from development to the staging environment
- D. Replacing a failed power supply in the core router of the data center

**Answer: B**

#### Explanation:

Choices A and C are processing events which may impact performance, but would not cause downtime. Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenance activities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

#### NEW QUESTION 473

- (Topic 5)

A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

- A. concurrent acces
- B. deadlock
- C. unauthorized access to dat
- D. a loss of data integrit

**Answer: D**

#### Explanation:

Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

#### NEW QUESTION 476

- (Topic 5)

Which of the following is widely accepted as one of the critical components in networking management?

- A. Configuration management
- B. Topological mappings
- C. Application of monitoring tools
- D. Proxy server troubleshooting

**Answer: A**

#### Explanation:

Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally, it also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server troubleshooting is used for troubleshooting purposes.

#### NEW QUESTION 480

- (Topic 5)

An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?

- A. Analyze the need for the structural chang
- B. Recommend restoration to the originally designed structur
- C. Recommend the implementation of a change control proces
- D. Determine if the modifications were properly approve

**Answer: D**

#### Explanation:

An IS auditor should first determine if the modifications were properly approved. Choices A, B and C are possible subsequent actions, should the IS auditor find that the structural modification had not been approved.

#### NEW QUESTION 484

- (Topic 5)

The purpose of code signing is to provide assurance that:

- A. the software has not been subsequently modifie



- B. the application can safely interface with another signed applicatio
- C. the signer of the application is trustee
- D. the private key of the signer has not been compromise

**Answer:** A

**Explanation:**

Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

#### NEW QUESTION 487

- (Topic 5)

An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

- A. apply the patch according to the patch's release note
- B. ensure that a good change management process is in plac
- C. thoroughly test the patch before sending it to productio
- D. approve the patch after doing a risk assessmen

**Answer:** B

**Explanation:**

An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly. The other choices are part of a good change management process but are not an IS auditor's responsibility.

#### NEW QUESTION 491

- (Topic 5)

The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?

- A. Rewrite the patches and apply them
- B. Code review and application of available patches
- C. Develop in-house patches
- D. identify and test suitable patches before applying them

**Answer:** D

**Explanation:**

Suitable patches from the existing developers should be selected and tested before applying them. Rewriting the patches and applying them is not a correct answer because it would require skilled resources and time to rewrite the patches. Code review could be possible but tests need to be performed before applying the patches. Since the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.

#### NEW QUESTION 492

- (Topic 5)

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- A. improve internal control procedure
- B. harden the network to industry best practice
- C. highlight the importance of incident response management to managemen
- D. improve employee awareness of the incident response proces

**Answer:** A

**Explanation:**

A postincident review examines both the cause and response to an incident. The lessons learned from the review can be used to improve internal controls. Understanding the purpose and structure of postincident reviews and follow-up procedures enable the information security manager to continuously improve the security program. Improving the incident response plan based on the incident review is an internal (corrective) control. The network may already be hardened to industry best practices. Additionally, the network may not be the source of the incident. The primary objective is to improve internal control procedures, not to highlight the importance of incident response management (IRM), and an incident response (IR) review does not improve employee awareness.

#### NEW QUESTION 495

- (Topic 5)

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- A. compromises the Wireless Application Protocol (WAP) gatewa
- B. installs a sniffing program in front of the serve
- C. steals a customer's PD
- D. listens to the wireless transmissio

**Answer:** A

**Explanation:**

In a WAP gateway, the encrypted messages from customers must be decrypted to transmit over the Internet and vice versa. Therefore, if the gateway is compromised, all of the messages would be exposed. SSL protects the messages from sniffing on the Internet, limiting disclosure of the customer's information. WTLS provides authentication, privacy and integrity and prevents messages from eavesdropping.

#### NEW QUESTION 496

- (Topic 5)

An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- A. Electromagnetic interference (EMI)
- B. Cross-talk
- C. Dispersion
- D. Attenuation

**Answer:** D

#### Explanation:

Attenuation is the weakening of signals during transmission. When the signal becomes weak, it begins to read a 1 for a 0, and the user may experience communication problems. UTP faces attenuation around 100 meters. Electromagnetic interference (EMI) is caused by outside electromagnetic waves affecting the desired signals, which is not the case here. Cross-talk has nothing to do with the length of the UTP cable.

#### NEW QUESTION 501

- (Topic 5)

Which of the following line media would provide the BEST security for a telecommunication network?

- A. Broadband network digital transmission
- B. Baseband network
- C. Dial-up
- D. Dedicated lines

**Answer:** D

#### Explanation:

Dedicated lines are set apart for a particular user or organization. Since there is no sharing of lines or intermediate entry points, the risk of interception or disruption of telecommunications messages is lower.

#### NEW QUESTION 506

- (Topic 5)

Neural networks are effective in detecting fraud because they can:

- A. discover new trends since they are inherently linear
- B. solve problems where large and general sets of training data are not obtainable
- C. attack problems that require consideration of a large number of input variables
- D. make assumptions about the shape of any curve relating variables to the output

**Answer:** C

#### Explanation:

Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

#### NEW QUESTION 507

- (Topic 5)

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- A. address of the domain server
- B. resolution service for the name/address
- C. IP addresses for the internet
- D. domain name system

**Answer:** B

#### Explanation:

DNS is utilized primarily on the Internet for resolution of the name/address of the web site. It is an Internet service that translates domain names into IP addresses. As names are alphabetic, they are easier to remember. However, the Internet is based on IP addresses. Every time a domain name is used, a DNS service must translate the name into the corresponding IP address. The DNS system has its own network, if one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

#### NEW QUESTION 509

- (Topic 5)

In what way is a common gateway interface (CGI) MOST often used on a webserver?



- A. Consistent way for transferring data to the application program and back to the user
- B. Computer graphics imaging method for movies and TV
- C. Graphic user interface for web design
- D. interface to access the private gateway domain

**Answer:** A

**Explanation:**

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word or entering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

**NEW QUESTION 512**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 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 First Try
- \* CISA Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The CISA Practice Test Here](#)**