



**Isaca**

## **Exam Questions CISA**

Isaca CISA

#### NEW QUESTION 1

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 2

- (Topic 1)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 3

- (Topic 1)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 4

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 5

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

**NEW QUESTION 6**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

**NEW QUESTION 7**

- (Topic 1)

A LAN administrator normally would be restricted from:

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

**Answer: C**

**Explanation:**

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

**NEW QUESTION 8**

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

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

**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 manual
- B. performance of a comprehensive security control review by the IS auditor
- C. adoption of a corporate information security policy statement
- D. purchase of security access control software

**Answer: C**

**Explanation:**

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

**NEW QUESTION 10**

- (Topic 1)

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

- A. logic bomb
- B. stealth virus

- C. trojan hors
- D. polymorphic viru

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 10

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 13

- (Topic 1)

IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

- A. True
- B. False

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 16

- (Topic 1)

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

- A. Controls testing starts earlie
- B. Auditing resources are allocated to the areas of highest concer
- C. Auditing risk is reduce
- D. Controls testing is more thorough

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 20

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 23

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 24**

- (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 28**

- (Topic 1)

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

- A. True
- B. False

**Answer:** B

**Explanation:**

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

**NEW QUESTION 31**

- (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 35**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 40**

- (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 45**

- (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 47**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 48**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 51**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 54**

- (Topic 1)

Why does the IS auditor often review the system logs?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 59**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 61**

- (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 66**

- (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 69**

- (Topic 1)

How does the SSL network protocol provide confidentiality?

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

**Answer: D**

**Explanation:**

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

**NEW QUESTION 71**

- (Topic 1)

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

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

**Answer: C**

**Explanation:**

PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

**NEW QUESTION 73**

- (Topic 1)

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

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

**Answer: A**

**Explanation:**

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

#### NEW QUESTION 78

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

#### NEW QUESTION 79

- (Topic 1)

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

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

**Answer: D**

#### Explanation:

Biometrics can be used to provide excellent physical access control.

#### NEW QUESTION 80

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

Data diddling involves modifying data before or during systems data entry.

#### NEW QUESTION 83

- (Topic 1)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 84

- (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 89

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 93**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

A primary high-level goal for an auditor who is reviewing a systems-development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

**NEW QUESTION 98**

- (Topic 1)

Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

- A. True
- B. False

**Answer:** B

**Explanation:**

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

**NEW QUESTION 101**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 102**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 104**

- (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 107

- (Topic 1)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 111

- (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 112

- (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 116

- (Topic 1)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 118

- (Topic 1)

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

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 120

- (Topic 1)

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

- A. Security policy administrators
- B. Business unit management

- C. Senior management
- D. Board of directors

**Answer:** B

**Explanation:**

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

**NEW QUESTION 121**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

When auditing third-party service providers, an auditor should be concerned with ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster.

**NEW QUESTION 123**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 125**

- (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 128**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 133**

- (Topic 1)

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

- A. WAP is often configured by default settings and is thus insecure
- B. WAP provides weak encryption for wireless traffic
- C. WAP functions as a protocol-conversion gateway for wireless TLS to Internet SS
- D. WAP often interfaces critical IT system

**Answer:** C

**Explanation:**

Functioning as a protocol-conversion gateway for wireless TLS to Internet SSL, the WAP gateway is a component warranting critical concern and review for the IS

auditor when auditing and testing controls that enforce message confidentiality.

#### NEW QUESTION 135

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

Modems (modulation/demodulation) convert analog transmissions to digital, and digital transmissions to analog, and are required for analog transmissions to enter a digital network.

#### NEW QUESTION 140

- (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 145

- (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 147

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 152

- (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 156

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

Authentication is used to validate a subject's identity.

**NEW QUESTION 160**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 165**

- (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 166**

- (Topic 1)

Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

- A. True
- B. False

**Answer:** B

**Explanation:**

Instead of simply reviewing the effectiveness and utilization of assets, an IS auditor is more concerned with adequate access control, appropriate access policies, and effectiveness of safeguards and procedures.

**NEW QUESTION 168**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 171**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 176**

- (Topic 1)

What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

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

**Answer:** D

**Explanation:**

Regression testing should use data from previous tests to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors.

**NEW QUESTION 178**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 183**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 187**

- (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 192**

- (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 196**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

Transaction authorization is the primary security concern for EDI environments.

**NEW QUESTION 199**

- (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 203**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 206**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

Hash totals are used as a control to detect loss, corruption, or duplication of data.

**NEW QUESTION 210**

- (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 212**

- (Topic 1)

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

- A. Substantive
- B. Compliance

- C. Integrated
- D. Continuous audit

**Answer:** A

**Explanation:**

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

**NEW QUESTION 213**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 214**

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 219**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 223**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 227

- (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 230

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

ISACA auditing standards require that an IS auditor plan the audit work to address the audit objectives. Choice B is incorrect because the auditor does not collect evidence in the planning stage of an audit. Choices C and D are incorrect because they are not the primary goals of audit planning. The activities described in choices B, C and D are all undertaken to address audit objectives and are thus secondary to choice A.

#### NEW QUESTION 234

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 239

- (Topic 2)

An IS auditor evaluating logical access controls should FIRST:

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

**Answer:** D

#### Explanation:

When evaluating logical access controls, an IS auditor should first obtain an understanding of the security risks facing information processing by reviewing relevant documentation, by inquiries, and by conducting a risk assessment. Documentation and evaluation is the second step in assessing the adequacy, efficiency and effectiveness, thus identifying deficiencies or redundancy in controls. The third step is to test the access paths to determine if the controls are functioning. Lastly, the IS auditor evaluates the security environment to assess its adequacy by reviewing the written policies, observing practices and comparing them to appropriate security best practices.

#### NEW QUESTION 240

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 241**

- (Topic 2)

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

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

**Answer:** D

**Explanation:**

Exploitation of a known user ID and password requires minimal technical knowledge and exposes the network resources to exploitation. The technical barrier is low and the impact can be very high; therefore, the fact that many user IDs have identical passwords represents the greatest threat. External modems represent a security risk, but exploitation still depends on the use of a valid user account. While the impact of users installing software on their desktops can be high (for example, due to the installation of Trojans or key-logging programs), the likelihood is not high due to the level of technical knowledge required to successfully penetrate the network. Although network monitoring can be a useful detective control, it will only detect abuse of user accounts in special circumstances and is, therefore, not a first line of defense.

**NEW QUESTION 245**

- (Topic 2)

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 247**

- (Topic 2)

When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

**Answer:** A

**Explanation:**

An IS auditor should focus on when controls are exercised as data flow through a computer system. Choice B is incorrect since corrective controls may also be relevant. Choice C is incorrect, since corrective controls remove or reduce the effects of errors or irregularities and are exclusively regarded as compensating controls. Choice D is incorrect and irrelevant since the existence and function of controls is important, not the classification.

**NEW QUESTION 251**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

By observing the IS staff performing their tasks, an IS auditor can identify whether they are performing any incompatible operations, and by interviewing the IS staff, the auditor can get an overview of the tasks performed. Based on the observations and interviews the auditor can evaluate the segregation of duties. Management may not be aware of the detailed functions of each employee in the IS department; therefore, discussion with the management would provide only limited information regarding segregation of duties. An organization chart would not provide details of the functions of the employees. Testing of user rights would provide information about the rights they have within the IS systems, but would not provide complete information about the functions they perform.

#### **NEW QUESTION 253**

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

#### **NEW QUESTION 257**

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

#### **NEW QUESTION 260**

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

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

#### **NEW QUESTION 265**

- (Topic 2)

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

- A. topology diagram
- B. bandwidth usage
- C. traffic analysis report
- D. bottleneck location

**Answer:** A

**Explanation:**

The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

#### NEW QUESTION 269

- (Topic 2)

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

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

**Answer: B**

#### Explanation:

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

#### NEW QUESTION 274

- (Topic 2)

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

- A. confirm that the auditors did not overlook any important issue
- B. gain agreement on the finding
- C. receive feedback on the adequacy of the audit procedure
- D. test the structure of the final presentation

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 279

- (Topic 2)

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

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

**Answer: C**

#### Explanation:

An automated code comparison is the process of comparing two versions of the same program to determine whether the two correspond. It is an efficient technique because it is an automated procedure. Test data runs permit the auditor to verify the processing of preselected transactions, but provide no evidence about unexercised portions of a program. Code review is the process of reading program source code listings to determine whether the code contains potential errors or inefficient statements. A code review can be used as a means of code comparison but it is inefficient. The review of code migration procedures would not detect program changes.

#### NEW QUESTION 284

- (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 288

- (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 289**

- (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 294**

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 295**

- (Topic 2)

An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 297**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

auditor.

#### NEW QUESTION 302

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 306

- (Topic 3)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 308

- (Topic 3)

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

- A. business plan
- B. audit plan
- C. security plan
- D. investment plan

**Answer:** A

#### Explanation:

To govern IT effectively, IT and business should be moving in the same direction, requiring that the IT plans are aligned with an organization's business plans. The audit and investment plans are not part of the IT plan, while the security plan should be at a corporate level.

#### NEW QUESTION 311

- (Topic 3)

IT governance is PRIMARILY the responsibility of the:

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 312

- (Topic 3)

Which of the following IT governance best practices improves strategic alignment?

- A. Supplier and partner risks are managed
- B. A knowledge base on customers, products, markets and processes is in place
- C. A structure is provided that facilitates the creation and sharing of business information

D. Top management mediate between the imperatives of business and technolog

**Answer:** D

**Explanation:**

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets and processes being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

#### NEW QUESTION 316

- (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 317

- (Topic 3)

The ultimate purpose of IT governance is to:

- A. encourage optimal use of I
- B. reduce IT cost
- C. decentralize IT resources across the organizatio
- D. centralize control of I

**Answer:** A

**Explanation:**

IT governance is intended to specify the combination of decision rights and accountability that is best for the enterprise. It is different for every enterprise. Reducing IT costs may not be the best IT governance outcome for an enterprise. Decentralizing IT resources across the organization is not always desired, although it may be desired in a decentralized environment. Centralizing control of IT is not always desired. An example of where it might be desired is an enterprise desiring a single point of customer contact.

#### NEW QUESTION 319

- (Topic 3)

Responsibility for the governance of IT should rest with the:

- A. IT strategy committe
- B. chief information officer (CIO).
- C. audit committe
- D. board of director

**Answer:** D

**Explanation:**

Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly. The audit committee, the chief information officer (CIO) and the IT strategy committee all play a significant role in the successful implementation of IT governance within an organization, but the ultimate accountability resides with the board of directors.

#### NEW QUESTION 320

- (Topic 3)

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- A. User acceptance testing (UAT) occur for all reports before release into production
- B. Organizational data governance practices be put in place
- C. Standard software tools be used for report development
- D. Management sign-off on requirements for new reports

**Answer:** B

**Explanation:**

This choice directly addresses the problem. An organizationwide approach is needed to achieve effective management of data assets. This includes enforcing

standard definitions of data elements, which is part of a data governance initiative. The other choices, while sound development practices, do not address the root cause of the problem described.

#### NEW QUESTION 323

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 324

- (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 relationships

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 328

- (Topic 3)

An IS auditor should be concerned when a telecommunication analyst:

- A. monitors systems performance and tracks problems resulting from program change
- B. reviews network load requirements in terms of current and future transaction volume
- C. assesses the impact of the network load on terminal response times and network data transfer rate
- D. recommends network balancing procedures and improvements

**Answer: A**

#### Explanation:

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes (choice B), assessing the impact of network load or terminal response times and network data transfer rates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes (choice A) would put the analyst in a self-monitoring role.

#### NEW QUESTION 332

- (Topic 3)

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

- A. dependency on a single person
- B. inadequate succession planning
- C. one person knowing all parts of a system
- D. a disruption of operation

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 336

- (Topic 3)

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

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

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 340

- (Topic 3)

Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

- A. Deleting database activity logs
- B. Implementing database optimization tools
- C. Monitoring database usage
- D. Defining backup and recovery procedures

**Answer: A**

**Explanation:**

Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

#### NEW QUESTION 343

- (Topic 3)

To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

- A. enterprise data mode
- B. IT balanced scorecard (BSC).
- C. IT organizational structur
- D. historical financial statement

**Answer: B**

**Explanation:**

The IT balanced scorecard (BSC) is a tool that provides the bridge between IT objectives and business objectives by supplementing the traditional financial evaluation with measures to evaluate customer satisfaction, internal processes and the ability to innovate. An enterprise data model is a document defining the data structure of an organization and how data interrelate. It is useful, but it does not provide information on investments. The IT organizational structure provides an overview of the functional and reporting relationships in an IT entity. Historical financial statements do not provide information about planning and lack sufficient detail to enable one to fully understand management's activities regarding IT assets. Past costs do not necessarily reflect value, and assets such as data are not represented on the books of accounts.

#### NEW QUESTION 348

- (Topic 3)

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

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

**Answer: C**

**Explanation:**

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

#### NEW QUESTION 349

- (Topic 3)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 353**

- (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 354**

- (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 analysis
- C. an IT balanced scorecard
- D. business process reengineering

**Answer:** C

**Explanation:**

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

**NEW QUESTION 359**

- (Topic 3)

When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

- A. incorporates state of the art technology
- B. addresses the required operational controls
- C. articulates the IT mission and vision
- D. specifies project management practices

**Answer:** C

**Explanation:**

The IT strategic plan must include a clear articulation of the IT mission and vision. The plan need not address the technology, operational controls or project management practices.

**NEW QUESTION 361**

- (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 objectives
- B. actions to reduce hardware procurement costs
- C. a listing of approved suppliers of IT contract resources
- D. a description of the technical architecture for the organization's network perimeter security

**Answer:** A

**Explanation:**

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is 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 364

- (Topic 3)

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- A. are developed for the organization as a whole
- B. are more likely to be derived as a result of a risk assessment
- C. will not conflict with overall corporate policy
- D. ensure consistency across the organization

**Answer: B**

#### Explanation:

A bottom-up approach begins by defining operational-level requirements and policies, which are derived and implemented as the result of risk assessments. Enterprise-level policies are subsequently developed based on a synthesis of existing operational policies. Choices A, C and D are advantages of a top-down approach for developing organizational policies. This approach ensures that the policies will not be in conflict with overall corporate policy and ensure consistency across the organization.

#### NEW QUESTION 365

- (Topic 3)

The PRIMARY objective of an audit of IT security policies is to ensure that:

- A. they are distributed and available to all staff
- B. security and control policies support business and IT objectives
- C. there is a published organizational chart with functional descriptions
- D. duties are appropriately segregated

**Answer: B**

#### Explanation:

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

#### NEW QUESTION 368

- (Topic 3)

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- A. Response
- B. Correction
- C. Detection
- D. Monitoring

**Answer: A**

#### Explanation:

A sound IS security policy will most likely outline a response program to handle suspected intrusions. Correction, detection and monitoring programs are all aspects of information security, but will not likely be included in an IS security policy statement.

#### NEW QUESTION 370

- (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 374

- (Topic 3)

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

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

**Answer:**

C

**Explanation:**

A policy statement reflects the intent and support provided by executive management for proper security and establishes a starting point for developing the security program.

**NEW QUESTION 376**

- (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 378**

- (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 380**

- (Topic 3)

When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

- A. There could be a question regarding the legal jurisdiction
- B. Having a provider abroad will cause excessive costs in future audit
- C. The auditing process will be difficult because of the distance
- D. There could be different auditing norms

**Answer: A**

**Explanation:**

In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

**NEW QUESTION 383**

- (Topic 3)

An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

- A. References from other customers
- B. Service level agreement (SLA) template
- C. Maintenance agreement
- D. Conversion plan

**Answer: A**

**Explanation:**

An IS auditor should look for an independent verification that the ISP can perform the tasks being contracted for. References from other customers would provide an independent, external review and verification of procedures and processes the ISP follows-issues which would be of concern to an IS auditor. Checking references is a means of obtaining an independent verification that the vendor can perform the services it says it can. A maintenance agreement relates more to equipment than to services, and a conversion plan, while important, is less important than verification that the ISP can provide the services they propose.

#### NEW QUESTION 388

- (Topic 3)

When an organization is outsourcing their information security function, which of the following should be kept in the organization?

- A. Accountability for the corporate security policy
- B. Defining the corporate security policy
- C. Implementing the corporate security policy
- D. Defining security procedures and guidelines

**Answer:** A

#### Explanation:

Accountability cannot be transferred to external parties. Choices B, C and D can be performed by outside entities as long as accountability remains within the organization.

#### NEW QUESTION 392

- (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 393

- (Topic 3)

Which of the following is the BEST information source for management to use as an aid in the identification of assets that are subject to laws and regulations?

- A. Security incident summaries
- B. Vendor best practices
- C. CERT coordination center
- D. Significant contracts

**Answer:** D

#### Explanation:

Contractual requirements are one of the sources that should be consulted to identify the requirements for the management of information assets. Vendor best practices provides a basis for evaluating how competitive an enterprise is, while security incident summaries are a source for assessing the vulnerabilities associated with the IT infrastructure. CERT ([www.cert.org](http://www.cert.org)) is an information source for assessing vulnerabilities within the IT infrastructure.

#### NEW QUESTION 396

- (Topic 3)

Which of the following is a mechanism for mitigating risks?

- A. Security and control practices
- B. Property and liability insurance
- C. Audit and certification
- D. Contracts and service level agreements (SLAs)

**Answer:** A

#### Explanation:

Risks are mitigated by implementing appropriate security and control practices. Insurance is a mechanism for transferring risk. Audit and certification are mechanisms of risk assurance, while contracts and SLAs are mechanisms of risk allocation.

#### NEW QUESTION 397

- (Topic 3)

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

- A. vulnerabilities

- B. threat
- C. probability
- 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 402**

- (Topic 3)

An IS auditor is reviewing an IT security risk management program. Measures of security risk should:

- A. address all of the network risk
- B. be tracked over time against the IT strategic plan
- C. take into account the entire IT environment
- D. result in the identification of vulnerability tolerance

**Answer:** C

**Explanation:**

When assessing IT security risk, it is important to take into account the entire IT environment. Measures of security risk should focus on those areas with the highest criticality so as to achieve maximum risk reduction at the lowest possible cost. IT strategic plans are not granular enough to provide appropriate measures. Objective metrics must be tracked over time against measurable goals, thus the management of risk is enhanced by comparing today's results against last week, last month, last quarter. Risk measures will profile assets on a network to objectively measure vulnerability risk. They do not identify tolerances.

**NEW QUESTION 403**

- (Topic 3)

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

- A. performance measurement
- B. strategic alignment
- C. value delivery
- D. resource management

**Answer:** A

**Explanation:**

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

**NEW QUESTION 407**

- (Topic 3)

The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

- A. alignment of the IT activities with IS audit recommendation
- B. enforcement of the management of security risk
- C. implementation of the chief information security officer's (CISO) recommendation
- D. reduction of the cost for IT security

**Answer:** B

**Explanation:**

The major benefit of implementing a security program is management's assessment of risk and its mitigation to an appropriate level of risk, and the monitoring of the remaining residual risks. Recommendations, visions and objectives of the auditor and the chief information security officer (CISO) are usually included within a security program, but they would not be the major benefit. The cost of IT security may or may not be reduced.

**NEW QUESTION 412**

- (Topic 3)

An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

- A. Stricter controls should be implemented by both the organization and the cleaning agency
- B. No action is required since such incidents have not occurred in the past
- C. A clear desk policy should be implemented and strictly enforced in the organization
- D. A sound backup policy for all important office documents should be implemented

**Answer:** A

**Explanation:**

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

#### NEW QUESTION 416

- (Topic 3)

The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

- A. financial result
- B. customer satisfactio
- C. internal process efficienc
- D. innovation capacit

**Answer:** A

#### Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

#### NEW QUESTION 420

- (Topic 4)

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- A. effectiveness of the QA function because it should interact between project management and user management
- B. efficiency of the QA function because it should interact with the project implementation tea
- C. effectiveness of the project manager because the project manager should interact with the QA functio
- D. efficiency of the project manager because the QA function will need to communicate with the project implementation tea

**Answer:** A

#### Explanation:

To be effective the quality assurance (QA) function should be independent of project management. The QA function should never interact with the project implementation team since this can impact effectiveness. The project manager does not interact with the QA function, which should not impact the effectiveness of the project manager. The QA function does not interact with the project implementation team, which should not impact the efficiency of the project manager.

#### NEW QUESTION 421

- (Topic 4)

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

- A. increases in quality can be achieved, even if resource allocation is decrease
- B. increases in quality are only achieved if resource allocation is increase
- C. decreases in delivery time can be achieved, even if resource allocation is decrease
- D. decreases in delivery time can only be achieved if quality is decrease

**Answer:** A

#### Explanation:

The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

#### NEW QUESTION 422

- (Topic 4)

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- A. Report that the organization does not have effective project managemen
- B. Recommend the project manager be change
- C. Review the IT governance structur
- D. Review the conduct of the project and the business cas

**Answer:** D

#### Explanation:

Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound IT governance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

#### NEW QUESTION 426

- (Topic 4)

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

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

**Answer: B**

#### Explanation:

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

#### NEW QUESTION 430

- (Topic 4)

An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

- A. Project sponsor
- B. System development project team (SDPT)
- C. Project steering committee
- D. User project team (UPT)

**Answer: C**

#### Explanation:

A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

#### NEW QUESTION 432

- (Topic 4)

A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

- A. recommend that the project be halted until the issues are resolved
- B. recommend that compensating controls be implemented
- C. evaluate risks associated with the unresolved issue
- D. recommend that the project manager reallocate test resources to resolve the issue

**Answer: C**

#### Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choices might be appropriate only after the risks have been assessed.

#### NEW QUESTION 437

- (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 440

- (Topic 4)

Before implementing controls, management should FIRST ensure that the controls:

- A. satisfy a requirement in addressing a risk issue
- B. do not reduce productivity
- C. are based on a cost-benefit analysis

D. are detective or correctiv

**Answer:** A

**Explanation:**

When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

#### NEW QUESTION 442

- (Topic 4)

Information for detecting unauthorized input from a terminal would be BEST provided by the:

- A. console log printou
- B. transaction journa
- C. automated suspense file listin
- D. user error repor

**Answer:** B

**Explanation:**

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error occurred, while the user error report would only list input that resulted in an edit error.

#### NEW QUESTION 443

- (Topic 4)

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

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

**Answer:** C

**Explanation:**

A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteriA. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

#### NEW QUESTION 446

- (Topic 4)

The editing/validation of data entered at a remote site would be performed MOST effectively at the:

- A. central processing site after running the application syste
- B. central processing site during the running of the application syste
- C. remote processing site after transmission of the data to the central processing sit
- D. remote processing site prior to transmission of the data to the central processing sit

**Answer:** D

**Explanation:**

It is important that the data entered from a remote site is edited and validated prior to transmission to the central processing site.

#### NEW QUESTION 447

- (Topic 4)

Functional acknowledgements are used:

- A. as an audit trail for EDI transaction
- B. to functionally describe the IS departmen
- C. to document user roles and responsibilitie
- D. as a functional description of application softwar

**Answer:** A

**Explanation:**

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

#### NEW QUESTION 448

- (Topic 4)

What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

- A. Test data/deck
- B. Base-case system evaluation
- C. Integrated test facility (ITF)
- D. Parallel simulation

**Answer: B**

#### Explanation:

A base-case system evaluation uses test data sets developed as part of comprehensive testing programs, it is used to verify correct systems operations before acceptance, as well as periodic validation. Test data/deck simulates transactions through real programs. An ITF creates fictitious files in the database with test transactions processed simultaneously with live input. Parallel simulation is the production of data processed using computer programs that simulate application program logic.

#### NEW QUESTION 452

- (Topic 4)

An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

- A. acknowledge receipt of electronic orders with a confirmation message
- B. perform reasonableness checks on quantities ordered before filling order
- C. verify the identity of senders and determine if orders correspond to contract terms
- D. encrypt electronic order

**Answer: C**

#### Explanation:

An electronic data interchange (EDI) system is subject not only to the usual risk exposures of computer systems but also to those arising from the potential ineffectiveness of controls on the part of the trading partner and the third-party service provider, making authentication of users and messages a major security concern. Acknowledging the receipt of electronic orders with a confirming message is good practice but will not authenticate orders from customers. Performing reasonableness checks on quantities ordered before placing orders is a control for ensuring the correctness of the company's orders, not the authenticity of its customers' orders. Encrypting sensitive messages is an appropriate step but does not apply to messages received.

#### NEW QUESTION 453

- (Topic 4)

During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

- A. test the software for compatibility with existing hardware
- B. perform a gap analysis
- C. review the licensing policies
- D. ensure that the procedure had been approved

**Answer: D**

#### Explanation:

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

#### NEW QUESTION 456

- (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 458

- (Topic 4)

Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

- A. inheritance
- B. Dynamic warehousing
- C. Encapsulation

D. Polymorphism

**Answer:** C

**Explanation:**

Encapsulation is a property of objects, and it prevents accessing either properties or methods that have not been previously defined as public. This means that any implementation of the behavior of an object is not accessible. An object defines a communication interface with the exterior and only that which belongs to that interface can be accessed.

**NEW QUESTION 461**

- (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 463**

- (Topic 4)

The use of object-oriented design and development techniques would MOST likely:

- A. facilitate the ability to reuse module
- B. improve system performance
- C. enhance control effectiveness
- D. speed up the system development life cycle

**Answer:** A

**Explanation:**

One of the major benefits of object-oriented design and development is the ability to reuse modules. The other options do not normally benefit from the object-oriented technique.

**NEW QUESTION 466**

- (Topic 4)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 467**

- (Topic 4)

The GREATEST benefit in implementing an expert system is the:

- A. capturing of the knowledge and experience of individuals in an organization
- B. sharing of knowledge in a central repository
- C. enhancement of personnel productivity and performance
- D. reduction of employee turnover in key departments

**Answer:** A

**Explanation:**

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit;

however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

#### NEW QUESTION 472

- (Topic 4)

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

- A. test data covering critical application
- B. detailed test plan
- C. quality assurance test specification
- D. user acceptance testing specification

**Answer:** D

#### Explanation:

A key objective in any software development project is to ensure that the developed software will meet the business objectives and the requirements of the user. The users should be involved in the requirements definition phase of a development project and user acceptance test specification should be developed during this phase. The other choices are generally performed during the system testing phase.

#### NEW QUESTION 475

- (Topic 4)

Which of the following is an advantage of the top-down approach to software testing?

- A. Interface errors are identified early
- B. Testing can be started before all programs are complete
- C. it is more effective than other testing approaches
- D. Errors in critical modules are detected sooner

**Answer:** A

#### Explanation:

The advantage of the top-down approach is that tests of major functions are conducted early, thus enabling the detection of interface errors sooner. The most effective testing approach is dependent on the environment being tested. Choices B and D are advantages of the bottom-up approach to system testing.

#### NEW QUESTION 478

- (Topic 4)

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

- A. Applications may not be subject to testing and IT general controls
- B. increased development and maintenance costs
- C. increased application development time
- D. Decision-making may be impaired due to diminished responsiveness to requests for information

**Answer:** A

#### Explanation:

End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls, quality assurance procedures, and documentation. A risk of end-user applications is that management may rely on them as much as traditional applications. End-user computing (EUC) systems typically result in reduced application development and maintenance costs, and a reduced development cycle time. EUC systems normally increase flexibility and responsiveness to management's information requests.

#### NEW QUESTION 479

- (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 480

- (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 483**

- (Topic 4)

Which of the following would impair the independence of a quality assurance team?

- A. Ensuring compliance with development methods
- B. Checking the testing assumptions
- C. Correcting coding errors during the testing process
- D. Checking the code to ensure proper documentation

**Answer:** C

**Explanation:**

Correction of code should not be a responsibility of the quality assurance team as it would not ensure segregation of duties and would impair the team's independence. The other choices are valid quality assurance functions.

**NEW QUESTION 488**

.....

## 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 FirstTry
- \* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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