

# Isaca

## Exam Questions CISA

Isaca CISA



#### NEW QUESTION 1

- (Topic 1)

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

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

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 2

- (Topic 1)

Which of the following is a benefit of using callback devices?

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

**Answer: A**

**Explanation:**

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

#### NEW QUESTION 3

- (Topic 1)

A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

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

**Answer: A**

**Explanation:**

A call-back system in a net centric environment would mean that a user with an id and password calls a remote server through a dial-up line first, and then the server disconnects and dials back to the user machine based on the user id and password using a telephone number from its database. Although the server can depend upon its own database, it cannot know the authenticity of the dialer when the user dials again. The server cannot depend upon the sender's database to dial back as the same could be manipulated.

#### NEW QUESTION 4

- (Topic 1)

Structured programming is BEST described as a technique that:

- A. provides knowledge of program functions to other programmers via peer review
- B. reduces the maintenance time of programs by the use of small-scale program module
- C. makes the readable coding reflect as closely as possible the dynamic execution of the progra
- D. controls the coding and testing of the high-level functions of the program in the development proces

**Answer: B**

**Explanation:**

A characteristic of structured programming is smaller, workable units. Structured programming has evolved because smaller, workable units are easier to maintain. Structured programming is a style of programming which restricts the kinds of control structures. This limitation is not crippling. Any program can be written with allowed control structures. Structured programming is sometimes referred to as go-to-less programming, since a go-to statement is not allowed. This is perhaps the most well known restriction of the style, since go-to statements were common at the time structured programming was becoming more popular. Statement labels also become unnecessary, except in languages where subroutines are identified by labels.

#### NEW QUESTION 5

- (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 6

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 7

- (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 8

- (Topic 1)

A database administrator is responsible for:

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 9

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 10

- (Topic 1)

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

- A. digest signatur
- B. electronic signatur
- C. digital signatur
- D. hash signatur

**Answer: C**

#### Explanation:

A digital signature through the private cryptographic key authenticates a transmission from a sender through the private cryptographic key. It is a string of bits that uniquely represent another string of bits, a digital document. An electronic signature refers to the string of bits that digitally represents a handwritten signature captured by a computer system when a human applies it on an electronic pen pad, connected to the system.

#### NEW QUESTION 10

- (Topic 1)

A hub is a device that connects:

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 11

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 12

- (Topic 1)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 14

- (Topic 1)

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST costeffective test of the DRP?

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

**Answer: B**

#### Explanation:

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery.

#### NEW QUESTION 15

- (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 17

- (Topic 1)

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

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

**Answer:** C

#### Explanation:

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

#### NEW QUESTION 19

- (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 23

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 24

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 29

- (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 32

- (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 33

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 36

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 39

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 42

- (Topic 1)

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

- A. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet



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

**Answer:** A

**Explanation:**

A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.

**NEW QUESTION 45**

- (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 46**

- (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 47**

- (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 49**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 54**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 57**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 61**

- (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 62**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 66**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 68**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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



#### NEW QUESTION 69

- (Topic 1)

What influences decisions regarding criticality of assets?

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

**Answer:** C

#### Explanation:

Criticality of assets is often influenced by the business criticality of the data to be protected and by the scope of the impact upon the organization as a whole. For example, the loss of a network backbone creates a much greater impact on the organization as a whole than the loss of data on a typical user's workstation.

#### NEW QUESTION 71

- (Topic 1)

Library control software restricts source code to:

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 74

- (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 79

- (Topic 1)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 81

- (Topic 1)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 86

- (Topic 1)

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

- A. Lack of IT documentation is not usually material to the controls tested in an IT audit
- B. The auditor should at least document the informal standards and policies
- C. Furthermore, the IS auditor should create formal documented policies to be implemented
- D. The auditor should at least document the informal standards and policies, and test for compliance
- E. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented
- F. The auditor should at least document the informal standards and policies, and test for compliance
- G. Furthermore, the IS auditor should create formal documented policies to be implemented

**Answer:** C

**Explanation:**

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

**NEW QUESTION 87**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 89**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 93**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 98**

- (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 102**

- (Topic 1)

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

- A. True

B. False

**Answer:** A

**Explanation:**

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

**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 110**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 113**

- (Topic 1)

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

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

**Answer:** D

**Explanation:**

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

**NEW QUESTION 115**

- (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)

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 120

- (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 122

- (Topic 1)

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

- A. True
- B. False

**Answer:** B

**Explanation:**

An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

#### NEW QUESTION 125

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 129

- (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 133

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 137**

- (Topic 1)

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

- A. Risk varie
- B. Risk is reduce
- C. Risk is not affecte
- D. Risk is increase

**Answer:** D

**Explanation:**

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

**NEW QUESTION 142**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 146**

- (Topic 1)

What are trojan horse programs? Choose the BEST answer.

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

**Answer:** D

**Explanation:**

Trojan horse programs are a common form of Internet attack.

**NEW QUESTION 147**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 149**

- (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 154**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 156**

- (Topic 1)

What is a callback system?

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 159**

- (Topic 1)

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

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

**Answer:** A

**Explanation:**

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

**NEW QUESTION 160**

- (Topic 1)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 163**

- (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 165**

- (Topic 1)

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

- A. Within five business days following installation



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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 170**

- (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 175**

- (Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 176**

- (Topic 1)

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

- A. True
- B. False

**Answer:** B

**Explanation:**

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

**NEW QUESTION 179**

- (Topic 1)

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

- A. True
- B. False

**Answer:** A

**Explanation:**

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

**NEW QUESTION 180**

- (Topic 1)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 184

- (Topic 1)

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

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

**Answer:** B

#### **Explanation:**

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

#### NEW QUESTION 189

- (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 190

- (Topic 1)

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

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

**Answer:** B

#### **Explanation:**

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

#### NEW QUESTION 194

- (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)

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

- A. True
- B. False

**Answer:** A

#### **Explanation:**

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

#### NEW QUESTION 198

- (Topic 1)

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

- A. Accuracy check
- B. Completeness check

- C. Reasonableness check
- D. Redundancy check

**Answer:** C

**Explanation:**

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

**NEW QUESTION 203**

- (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 208**

- (Topic 2)

Which of the following is a substantive test?

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

**Answer:** C

**Explanation:**

A substantive test confirms the integrity of actual processing. A substantive test would determine if the tape library records are stated correctly. A compliance test determines if controls are being applied in a manner that is consistent with management policies and procedures. Checking the authorization of exception reports, reviewing authorization for changing parameters and reviewing password history reports are all compliance tests.

**NEW QUESTION 212**

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 215**

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

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

**NEW QUESTION 219**

- (Topic 2)

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 222

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 226

- (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 networ
- B. Users can install software on their desktop
- C. Network monitoring is very limite
- D. Many user IDs have identical password

**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 231

- (Topic 2)

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

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

**Answer:** A

**Explanation:**

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

#### NEW QUESTION 235

CORRECT TEXT - (Topic 2)

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- A. Test data
- B. Generalized audit software
- C. Integrated test facility
- D. Embedded audit module

**Answer:** B

#### NEW QUESTION 236

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 239

- (Topic 2)

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

- A. A confirmation letter received from a third party verifying an account balance
- B. Assurance from line management that an application is working as designed
- C. Trend data obtained from World Wide Web (Internet) sources
- D. Ratio analysts developed by the IS auditor from reports supplied by line management

**Answer:** A

#### Explanation:

Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

#### NEW QUESTION 244

- (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 248

- (Topic 2)

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 253

- (Topic 2)

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



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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 257

- (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 261

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 265

- (Topic 2)

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

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 267

- (Topic 2)

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

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

**Answer:** B

**Explanation:**

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



#### NEW QUESTION 272

- (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 274

- (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 277

- (Topic 2)

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

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 279

- (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 280

- (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 283**

- (Topic 2)

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

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

**Answer: B**

**Explanation:**

Generalized audit software (GAS) would enable the auditor to review the entire invoice file to look for those items that meet the selection criteria. Attribute sampling would aid in identifying records meeting specific conditions, but would not compare one record to another to identify duplicates. To detect duplicate invoice records the IS auditor should check all of the items that meet the criteria and not just a sample of the items. Test data are used to verify program processing, but will not identify duplicate records. An integrated test facility (ITF) allows the IS auditor to test transactions through the production system, but would not compare records to identify duplicates.

**NEW QUESTION 287**

- (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 288**

- (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 292**

- (Topic 2)

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

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

**Answer: C**

**Explanation:**

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

#### NEW QUESTION 294

- (Topic 2)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 296

- (Topic 2)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 301

- (Topic 2)

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

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

**Answer: A**

#### Explanation:

CSA is predicated on the review of high-risk areas that either need immediate attention or a more thorough review at a later date. Choice B is incorrect, because CSA requires the involvement of auditors and line management. What occurs is that the internal audit function shifts some of the control monitoring responsibilities to the functional areas. Choice C is incorrect because CSA is not a replacement for traditional audits. CSA is not intended to replace audit's responsibilities, but to enhance them. Choice D is incorrect, because CSA does not allow management to relinquish its responsibility for controls.

#### NEW QUESTION 303

- (Topic 3)

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

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 307

- (Topic 3)

Which of the following is the MOST important element for the successful implementation of IT governance?

- A. Implementing an IT scorecard
- B. Identifying organizational strategies
- C. Performing a risk assessment
- D. Creating a formal security policy

**Answer:** B

**Explanation:**

The key objective of an IT governance program is to support the business, thus the identification of organizational strategies is necessary to ensure alignment between IT and corporate governance. Without identification of organizational strategies, the remaining choices—even if implemented—would be ineffective.

#### NEW QUESTION 312

- (Topic 3)

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

- A. IT budget
- B. existing IT environment
- C. business plan
- D. investment plan

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 315

- (Topic 3)

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- A. Repeatable but Intuitive
- B. Defined
- C. Managed and Measurable
- D. Optimized

**Answer:** B

**Explanation:**

Defined (level 3) is the lowest level at which an IT balanced scorecard is defined.

#### NEW QUESTION 318

- (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 322

- (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 improvement

**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 325

- (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 330

- (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 334

- (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 336

- (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 339

- (Topic 3)

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

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



**Answer:** A

**Explanation:**

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

#### NEW QUESTION 343

- (Topic 3)

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

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

**Answer:** D

**Explanation:**

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

#### NEW QUESTION 345

- (Topic 3)

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

- A. the existing IT environment
- B. the business plan
- C. the present IT budget
- D. current technology trend

**Answer:** B

**Explanation:**

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

#### NEW QUESTION 349

- (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 control
- C. articulates the IT mission and vision
- D. specifies project management practice

**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 351

- (Topic 3)

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

- A. an assessment of the fit of the organization's application portfolio with business objective
- B. actions to reduce hardware procurement 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 354



- (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 358

- (Topic 3)

An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- A. this lack of knowledge may lead to unintentional disclosure of sensitive information
- B. information security is not critical to all functions
- C. IS audit should provide security training to the employee
- D. the audit finding will cause management to provide continuous training to staff

**Answer: A**

**Explanation:**

All employees should be aware of the enterprise's information security policy to prevent unintentional disclosure of sensitive information. Training is a preventive control. Security awareness programs for employees can prevent unintentional disclosure of sensitive information to outsiders.

#### NEW QUESTION 360

- (Topic 3)

Which of the following should be included in an organization's IS security policy?

- A. A list of key IT resources to be secured
- B. The basis for access authorization
- C. Identity of sensitive security features
- D. Relevant software security features

**Answer: B**

**Explanation:**

The security policy provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

#### NEW QUESTION 365

- (Topic 3)

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

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

**Answer: D**

**Explanation:**

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

#### NEW QUESTION 366

- (Topic 3)

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- A. the IT infrastructure
- B. organizational policies, standards and procedure
- C. legal and regulatory requirements
- D. the adherence to organizational policies, standards and procedure

**Answer: C**

**Explanation:**

To ensure that the organization is complying with privacy issues, an IS auditor should address legal and regulatory requirements first. To comply with legal and regulatory requirements, organizations need to adopt the appropriate infrastructure. After understanding the legal and regulatory requirements, an IS auditor should evaluate organizational policies, standards and procedures to determine whether they adequately address the privacy requirements, and then review the adherence to these specific policies, standards and procedures.

#### NEW QUESTION 367

- (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 368

- (Topic 3)

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

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

**Answer: D**

#### Explanation:

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

#### NEW QUESTION 370

- (Topic 3)

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- A. enhanced reputation
- B. enhanced staff morale
- C. the use of new technology
- D. increased market penetration

**Answer: D**

#### Explanation:

A comprehensive business case for any proposed IT-related business investment should have clearly defined business benefits to enable the expected return to be calculated. These benefits usually fall into two categories: direct and indirect, or soft. Direct benefits usually comprise the quantifiable financial benefits that the new system is expected to generate. The potential benefits of enhanced reputation and enhanced staff morale are difficult to quantify, but should be quantified to the extent possible. IT investments should not be made just for the sake of new technology but should be based on a quantifiable business need.

#### NEW QUESTION 373

- (Topic 3)

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

- A. optimize security investments in support of business objective
- B. implement a standard set of security practices
- C. institute a standards-based solution
- D. implement a continuous improvement culture

**Answer: A**

#### Explanation:

In the context of effective information security governance, value delivery is implemented to ensure optimization of security investments in support of business objectives. The tools and techniques for implementing value delivery include implementation of a standard set of security practices, institutionalization and commoditization of standards-based solutions, and implementation of a continuous improvement culture considering security as a process, not an event.

#### NEW QUESTION 377

- (Topic 3)

Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

- A. Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary plan

- B. Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contract
- C. No, because the backup to be provided should be specified adequately in the contract
- D. No, because the service bureau's business continuity plan is proprietary information

**Answer:** A

**Explanation:**

The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

#### NEW QUESTION 382

- (Topic 3)

To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

- A. O/S and hardware refresh frequencies
- B. Gain-sharing performance bonuses
- C. Penalties for noncompliance
- D. Charges tied to variable cost metrics

**Answer:** B

**Explanation:**

Because the outsourcer will share a percentage of the achieved savings, gain-sharing performance bonuses provide a financial incentive to go above and beyond the stated terms of the contract and can lead to cost savings for the client. Refresh frequencies and penalties for noncompliance would only encourage the outsourcer to meet minimum requirements. Similarly, tying charges to variable cost metrics would not encourage the outsourcer to seek additional efficiencies that might benefit the client.

#### NEW QUESTION 383

- (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 387

- (Topic 3)

The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

- A. destruction policy
- B. security policy
- C. archive policy
- D. audit policy

**Answer:** C

**Explanation:**

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

#### NEW QUESTION 388

- (Topic 3)

The output of the risk management process is an input for making:

- A. business plan
- B. audit charter
- C. security policy decision
- D. software design decision

**Answer:** C

**Explanation:**

The risk management process is about making specific, security-related decisions, such as the level of acceptable risk. Choices A, B and D are not ultimate goals of the risk management process.

#### NEW QUESTION 392

- (Topic 3)

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

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

**Answer: C**

#### Explanation:

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

#### NEW QUESTION 393

- (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 395

- (Topic 3)

Assessing IT risks is BEST achieved by:

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

**Answer: A**

#### Explanation:

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

#### NEW QUESTION 398

- (Topic 4)

Many IT projects experience problems because the development time and/or resource requirements are underestimated. Which of the following techniques would provide the GREATEST assistance in developing an estimate of project duration?

- A. Function point analysis
- B. PERT chart
- C. Rapid application development
- D. Object-oriented system development

**Answer: B**

#### Explanation:

A PERT chart will help determine project duration once all the activities and the work involved with those activities are known. Function point analysis is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries, logical internal files, etc. While this will help determine the size of individual activities, it will not assist in determining project duration since there are many overlapping tasks. Rapid application development is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality, while object-oriented system development is the process of solution specification and modeling.

#### NEW QUESTION 400

- (Topic 4)

The reason for establishing a stop or freezing point on the design of a new system is to:

- A. prevent further changes to a project in process

- B. indicate the point at which the design is to be complete
- C. require that changes after that point be evaluated for cost-effectiveness
- D. provide the project management team with more control over the project design

**Answer:** C

**Explanation:**

Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.

#### NEW QUESTION 403

- (Topic 4)

When planning to add personnel to tasks imposing time constraints on the duration of a project, which of the following should be revalidated FIRST?

- A. The project budget
- B. The critical path for the project
- C. The length of the remaining tasks
- D. The personnel assigned to other tasks

**Answer:** B

**Explanation:**

Since adding resources may change the route of the critical path, the critical path must be reevaluated to ensure that additional resources will in fact shorten the project duration. Given that there may be slack time available on some of the other tasks not on the critical path, factors such as the project budget, the length of other tasks and the personnel assigned to them may or may not be affected.

#### NEW QUESTION 406

- (Topic 4)

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- A. complexity and risks associated with the project have been analyzed
- B. resources needed throughout the project have been determined
- C. project deliverables have been identified
- D. a contract for external parties involved in the project has been completed

**Answer:** A

**Explanation:**

Understanding complexity and risk, and actively managing these throughout a project are critical to a successful outcome. The other choices, while important during the course of the project, cannot be fully determined at the time the project is initiated, and are often contingent upon the risk and complexity of the project.

#### NEW QUESTION 407

- (Topic 4)

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

- A. stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plan
- B. accept the project manager's position as the project manager is accountable for the outcome of the project
- C. offer to work with the risk manager when one is appointed
- D. inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project

**Answer:** A

**Explanation:**

The majority of project risks can typically be identified before a project begins, allowing mitigation/avoidance plans to be put in place to deal with these risks. A project should have a clear link back to corporate strategy and tactical plans to support this strategy. The process of setting corporate strategy, setting objectives and developing tactical plans should include the consideration of risks. Appointing a risk manager is a good practice but waiting until the project has been impacted by risks is misguided. Risk management needs to be forward looking; allowing risks to evolve into issues that adversely impact the project represents a failure of risk management. With or without a risk manager, persons within and outside of the project team need to be consulted and encouraged to comment when they believe new risks have emerged or risk priorities have changed. The IS auditor has an obligation to the project sponsor and the organization to advise on appropriate project management practices. Waiting for the possible appointment of a risk manager represents an unnecessary and dangerous delay to implementing risk management.

#### NEW QUESTION 409

- (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 410

- (Topic 4)

A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

- A. what amount of progress against schedule has been achieved
- B. if the project budget can be reduced
- C. if the project could be brought in ahead of schedule
- D. if the budget savings can be applied to increase the project scope

**Answer:** A

**Explanation:**

Cost performance of a project cannot be properly assessed in isolation of schedule performance. Cost cannot be assessed simply in terms of elapsed time on a project. To properly assess the project budget position it is necessary to know how much progress has actually been made and, given this, what level of expenditure would be expected. It is possible that project expenditure appears to be low because actual progress has been slow. Until the analysis of project against schedule has been completed, it is impossible to know whether there is any reason to reduce budget, if the project has slipped behind schedule, then not only may there be no spare budget but it is possible that extra expenditure may be needed to retrieve the slippage. The low expenditure could actually be representative of a situation where the project is likely to miss deadlines rather than potentially come in ahead of time. If the project is found to be ahead of budget after adjusting for actual progress, this is not necessarily a good outcome because it points to flaws in the original budgeting process; and, as said above, until further analysis is undertaken, it cannot be determined whether any spare funds actually exist. Further, if the project is behind schedule, then adding scope may be the wrong thing to do.

#### NEW QUESTION 412

- (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 416

- (Topic 4)

A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

- A. validation control
- B. internal credibility check
- C. clerical control procedure
- D. automated systems balancing

**Answer:** D

**Explanation:**

Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checks are certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to summarize and compare inputs and outputs, an automated process is less susceptible to error.

#### NEW QUESTION 418

- (Topic 4)

What control detects transmission errors by appending calculated bits onto the end of each segment of data?

- A. Reasonableness check
- B. Parity check
- C. Redundancy check



D. Check digits

**Answer:** C

**Explanation:**

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of data. A reasonableness check compares data to predefined reasonability limits or occurrence rates established for the data. A parity check is a hardware control that detects data errors when data are read from one computer to another, from memory or during transmission. Check digits detect transposition and transcription errors.

#### NEW QUESTION 421

- (Topic 4)

Which of the following is the GREATEST risk when implementing a data warehouse?

- A. increased response time on the production systems
- B. Access controls that are not adequate to prevent data modification
- C. Data duplication
- D. Data that is not updated or current

**Answer:** B

**Explanation:**

Once the data is in a warehouse, no modifications should be made to it and access controls should be in place to prevent data modification. Increased response time on the production systems is not a risk, because a data warehouse does not impact production data. Based on data replication, data duplication is inherent in a data warehouse. Transformation of data from operational systems to a data warehouse is done at predefined intervals, and as such, data may not be current.

#### NEW QUESTION 424

- (Topic 4)

A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

- A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
- B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
- C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
- D. Reengineering the existing processing and redesigning the existing system

**Answer:** C

**Explanation:**

EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

#### NEW QUESTION 429

- (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 434

- (Topic 4)

A decision support system (DSS):

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

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 438

- (Topic 4)

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

- A. users may prefer to use contrived data for testing
- B. unauthorized access to sensitive data may result
- C. error handling and credibility checks may not be fully proven
- D. the full functionality of the new process may not necessarily be tested

**Answer: B**

#### Explanation:

Unless the data are sanitized, there is a risk of disclosing sensitive data.

#### NEW QUESTION 442

- (Topic 4)

Which of the following is the PRIMARY purpose for conducting parallel testing?

- A. To determine if the system is cost-effective
- B. To enable comprehensive unit and system testing
- C. To highlight errors in the program interfaces with files
- D. To ensure the new system meets user requirements

**Answer: D**

#### Explanation:

The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements. Parallel testing may show that the old system is, in fact, better than the new system, but this is not the primary reason. Unit and system testing are completed before parallel testing. Program interfaces with files are tested for errors during system testing.

#### NEW QUESTION 445

- (Topic 4)

The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

- A. rule
- B. decision tree
- C. semantic net
- D. dataflow diagram

**Answer: B**

#### Explanation:

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

#### NEW QUESTION 448

- (Topic 4)

During which of the following phases in system development would user acceptance test plans normally be prepared?

- A. Feasibility study
- B. Requirements definition
- C. implementation planning
- D. Postimplementation review

**Answer: B**

#### Explanation:

During requirements definition, the project team will be working with the users to define their precise objectives and functional needs. At this time, the users should be working with the team to consider and document how the system functionality can be tested to ensure it meets their stated needs. The feasibility study is too early for such detailed user involvement, and the implementation planning and postimplementation review phases are too late. An IS auditor should know at what point user testing should be planned to ensure it is most effective and efficient.

#### NEW QUESTION 451

- (Topic 4)

Which of the following should be included in a feasibility study for a project to implement an EDI process?

- A. The encryption algorithm format
- B. The detailed internal control procedures
- C. The necessary communication protocols
- D. The proposed trusted third-party agreement

**Answer: C**

**Explanation:**

Encryption algorithms, third-party agreements and internal control procedures are too detailed for this phase. They would only be outlined and any cost or performance implications shown. The communications protocols must be included, as there may be significant cost implications if new hardware and software are involved, and risk implications if the technology is new to the organization.

**NEW QUESTION 455**

- (Topic 4)

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

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

**Answer: B**

**Explanation:**

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

**NEW QUESTION 460**

- (Topic 4)

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

- A. increased maintenance
- B. improper documentation of testing
- C. inadequate functional testing
- D. delays in problem resolution

**Answer: C**

**Explanation:**

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

**NEW QUESTION 465**

- (Topic 4)

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

- A. facilitates user involvement
- B. allows early testing of technical features
- C. facilitates conversion to the new system
- D. shortens the development time frame

**Answer: D**

**Explanation:**

The greatest advantage of RAD is the shorter time frame for the development of a system. Choices A and B are true, but they are also true for the traditional systems development life cycle. Choice C is not necessarily always true.

**NEW QUESTION 470**

- (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 department

**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 474**

- (Topic 4)

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- A. A sufficient quantity of data for each test case
- B. Data representing conditions that are expected in actual processing
- C. Completing the test on schedule
- D. A random sample of actual data

**Answer:** B

**Explanation:**

Selecting the right kind of data is key in testing a computer system. The data should not only include valid and invalid data but should be representative of actual processing; quality is more important than quantity. It is more important to have adequate test data than to complete the testing on schedule. It is unlikely that a random sample of actual data would cover all test conditions and provide a reasonable representation of actual data.

#### NEW QUESTION 475

- (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 479

- (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 481

- (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 environmen
- 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 486

- (Topic 4)

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

- A. Consider feasibility of a separate user acceptance environment
- B. Schedule user testing to occur at a given time each day
- C. implement a source code version control tool
- D. Only retest high priority defects

**Answer:** A

**Explanation:**

A separate environment or environments is normally necessary for testing to be efficient and effective, and to ensure the integrity of production code, it is important that the development and testing code base be separate. When defects are identified they can be fixed in the development environment, without interrupting testing, before being migrated in a controlled manner to the test environment. A separate test environment can also be used as the final staging area from which code is migrated to production. This enforces a separation between development and production code. The logistics of setting up and refreshing customized test data is easier if a separate environment is maintained. If developers and testers are sharing the same environment, they have to work effectively at separate times of the day. It is unlikely that this would provide optimum productivity. Use of a source code control tool is a good practice, but it does not properly mitigate the lack of an appropriate testing environment. Even low priority fixes run the risk of introducing unintended results when combined with the rest of the system code. To prevent this, regular regression testing covering all code changes should occur. A separate test environment makes the logistics of regression testing easier to manage.

#### **NEW QUESTION 490**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions and Answers in PDF Format

### CISA Practice Exam Features:

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

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