

Exam Questions CISA

Isaca CISA

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



NEW QUESTION 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

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

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

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 4

Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

- A. Router
- B. Bridge
- C. Repeater
- D. Gateway

Answer: B

Explanation:

A bridge connects two separate networks to form a logical network (e.g., joining an ethernet and token network) and has the storage capacity to store frames and act as a storage and forward device. Bridges operate at the OSI data link layer by examining the media access control header of a data packet.

NEW QUESTION 5

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 6

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 7

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

- A. testing stag
- B. evaluation stag
- C. maintenance stag
- D. early stages of plannin

Answer: D

Explanation:

Company.com in the early stages of a BCP will incur the most significant level of program development effort, which will level out as the BCP moves into maintenance, testing and evaluation stages. It is during the planning stage that an IS auditor will play an important role in obtaining senior management's commitment to resources and assignment of BCP responsibilities.

NEW QUESTION 8

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

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

Answer: D

Explanation:

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

NEW QUESTION 9

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

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

Answer: C

Explanation:

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

NEW QUESTION 10

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 10

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 14

An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

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

Answer: D

Explanation:

A DBA only in rare instances should be mapping data elements from the data model to the internal schema (physical data storage definitions). To do so would eliminate data independence for application systems. Mapping of the data model occurs with the conceptual schema since the conceptual schema represents the enterprisewide view of data within an organization and is the basis for deriving an end-user department data model.

NEW QUESTION 19

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 23

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

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

Answer: D

Explanation:

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

NEW QUESTION 24

The use of a GANTT chart can:

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

Answer: A

Explanation:

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

NEW QUESTION 26

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

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

Answer: A

Explanation:

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

NEW QUESTION 27

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

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

Answer: C

Explanation:

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

NEW QUESTION 30

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 33

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- A. Paper test
- B. Post test
- C. Preparedness test
- D. Walk-through

Answer: C

Explanation:

A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments.

NEW QUESTION 34

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

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

Answer: B

Explanation:

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

NEW QUESTION 39

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

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

Answer: B

Explanation:

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

NEW QUESTION 42

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

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

Answer: A

Explanation:

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

NEW QUESTION 43

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

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

Answer: B

Explanation:

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

NEW QUESTION 45

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

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

Answer: C

Explanation:

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

NEW QUESTION 47

What is the primary objective of a control self-assessment (CSA) program?

- A. Enhancement of the audit responsibility
- B. Elimination of the audit responsibility
- C. Replacement of the audit responsibility
- D. Integrity of the audit responsibility

Answer: A

Explanation: Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

NEW QUESTION 48

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

- A. True
- B. False

Answer: A

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

NEW QUESTION 53

What is the PRIMARY purpose of audit trails?

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

Answer: C

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

NEW QUESTION 55

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 60

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 63

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 65

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 68

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

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

Answer: D

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

NEW QUESTION 71

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 72

An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

- A. Evidence collected through personal observation
- B. Evidence collected through systems logs provided by the organization's security administration
- C. Evidence collected through surveys collected from internal staff
- D. Evidence collected through transaction reports provided by the organization's IT administration

Answer: A

Explanation: An IS auditor usually places more reliance on evidence directly collected, such as through personal observation.

NEW QUESTION 73

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

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

Answer: B

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

NEW QUESTION 75

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

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

Answer: B

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

NEW QUESTION 78

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 80

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

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

Answer: B

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

NEW QUESTION 83

What are used as the framework for developing logical access controls?

- A. Information systems security policies
- B. Organizational security policies
- C. Access Control Lists (ACL)
- D. Organizational charts for identifying roles and responsibilities

Answer: A

Explanation: Information systems security policies are used as the framework for developing logical access controls.

NEW QUESTION 87

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 89

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 92

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

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

Answer: C

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

NEW QUESTION 94

Which of the following do digital signatures provide?

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

Answer: A

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

NEW QUESTION 96

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

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

Answer: A

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

NEW QUESTION 101

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

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

Answer: D

Explanation: Biometrics can be used to provide excellent physical access control.

NEW QUESTION 104

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

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

Answer: A

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

NEW QUESTION 109

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

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

Answer: C

Explanation: Of the three major types of BCP tests (paper, walk-through, and preparedness), a walk-through test requires only that representatives from each operational area meet to review the plan.

NEW QUESTION 111

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

- A. True
- B. False

Answer: A

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

NEW QUESTION 114

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following? Choose the BEST answer.

- A. IT strategic plan
- B. Business continuity plan
- C. Business impact analysis
- D. Incident response plan

Answer: B

Explanation: Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of a business continuity plan.

NEW QUESTION 116

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

- A. True
- B. False

Answer: A

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

NEW QUESTION 119

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

- A. In program development and change management
- B. In program feasibility studies
- C. In program development
- D. In change management

Answer: A

Explanation: Regression testing is used in program development and change management to determine whether new changes have introduced any errors in the remaining unchanged code.

NEW QUESTION 123

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

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

Answer: C

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

NEW QUESTION 127

Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

- A. Interface systems with other applications or systems
- B. The entire program, including any interface systems with other applications or systems
- C. All programs, including interface systems with other applications or systems
- D. Mission-critical functions and any interface systems with other applications or systems

Answer: B

Explanation: Whenever an application is modified, the entire program, including any interface systems with other applications or systems, should be tested to determine the full impact of the change.

NEW QUESTION 129

The quality of the metadata produced from a data warehouse is _____ in the warehouse's design. Choose the BEST answer.

- A. Often hard to determine because the data is derived from a heterogeneous data environment
- B. The most important consideration
- C. Independent of the quality of the warehoused databases
- D. Of secondary importance to data warehouse content

Answer: B

Explanation: The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

NEW QUESTION 134

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 139

When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

- A. True
- B. False

Answer: B

Explanation: When participating in a systems-development project, an IS auditor should also strive to ensure that adequate and complete documentation exists for all projects.

NEW QUESTION 141

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 145

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 146

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 150

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 154

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 159

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 161

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

- A. The data must be normalize
- B. The data must be validate
- C. The data must be parallel-teste
- D. The data must be synchronize

Answer: D

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

NEW QUESTION 164

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

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

Answer: B

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

NEW QUESTION 165

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 168

To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

- A. The business objectives of the organization
- B. The effect of segregation of duties on internal controls
- C. The point at which controls are exercised as data flows through the system
- D. Organizational control policies

Answer: C

Explanation: When evaluating the collective effect of preventive, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

NEW QUESTION 171

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 174

Which of the following is of greatest concern to the IS auditor?

- A. Failure to report a successful attack on the network
- B. Failure to prevent a successful attack on the network
- C. Failure to recover from a successful attack on the network
- D. Failure to detect a successful attack on the network

Answer: A

Explanation: Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

NEW QUESTION 175

If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

- A. To advise senior management
- B. To reassign job functions to eliminate potential fraud
- C. To implement compensating control
- D. Segregation of duties is an administrative control not considered by an IS auditor

Answer: A

Explanation: An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

NEW QUESTION 178

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

- A. Security policy administrators
- B. Business unit management
- C. Senior management
- D. Board of directors

Answer: B

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

NEW QUESTION 180

Why does an IS auditor review an organization chart?

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

Answer: C

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

NEW QUESTION 183

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 187

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

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

Answer: C

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

NEW QUESTION 192

Who should be responsible for network security operations?

- A. Business unit managers
- B. Security administrators
- C. Network administrators
- D. IS auditors

Answer: B

Explanation: Security administrators are usually responsible for network security operations.

NEW QUESTION 197

The directory system of a database-management system describes:

- A. The access method to the data
- B. The location of data AND the access method
- C. The location of data
- D. Neither the location of data NOR the access method

Answer: B

Explanation: The directory system of a database-management system describes the location of data and the access method.

NEW QUESTION 202

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- A. The data should be deleted and overwritten with binary 0
- B. The data should be demagnetize
- C. The data should be low-level formatte
- D. The data should be delete

Answer: B

Explanation: To properly protect against unauthorized disclosure of sensitive data, hard disks should be demagnetized before disposal or release.

NEW QUESTION 207

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

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

Answer: C

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

NEW QUESTION 210

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 215

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

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

Answer: C

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

NEW QUESTION 218

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

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

Answer: B

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

NEW QUESTION 220

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

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

Answer: C

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

NEW QUESTION 225

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 229

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 231

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

- A. False
- B. True

Answer: B

Explanation: Digital signatures require the sender to "sign" the data by encrypting the data with the sender's private key, to then be decrypted by the recipient using the sender's public key.

NEW QUESTION 233

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

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

Answer: A

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

NEW QUESTION 238

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 239

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

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

Answer: B

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

NEW QUESTION 244

What should IS auditors always check when auditing password files?

- A. That deleting password files is protected

- B. That password files are encrypted
- C. That password files are not accessible over the network
- D. That password files are archived

Answer: B

Explanation: IS auditors should always check to ensure that password files are encrypted.

NEW QUESTION 247

Which of the following is the most fundamental step in preventing virus attacks?

- A. Adopting and communicating a comprehensive antivirus policy
- B. Implementing antivirus protection software on users' desktop computers
- C. Implementing antivirus content checking at all network-to-Internet gateways
- D. Inoculating systems with antivirus code

Answer: A

Explanation: Adopting and communicating a comprehensive antivirus policy is the most fundamental step in preventing virus attacks. All other antivirus prevention efforts rely upon decisions established and communicated via policy.

NEW QUESTION 252

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

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

Answer: A

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

NEW QUESTION 254

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

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

Answer: D

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

NEW QUESTION 257

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 261

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

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

Answer: B

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

NEW QUESTION 264

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 265

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 267

Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

- A. Financial reporting
- B. Sales reporting
- C. Inventory reporting
- D. Transaction processing

Answer: D

Explanation: Off-site data storage should be kept synchronized when preparing for the recovery of timesensitive data such as that resulting from transaction processing.

NEW QUESTION 272

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

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

Answer: C

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

NEW QUESTION 276

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

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

Answer: D

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

NEW QUESTION 281

What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

- A. Assigning copyright to the organization
- B. Program back doors
- C. Source code escrow
- D. Internal programming expertise

Answer: C

Explanation: Source code escrow protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business.

NEW QUESTION 284

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

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

Answer: D

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

NEW QUESTION 285

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

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

Answer: A

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

NEW QUESTION 287

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

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

Answer: B

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

NEW QUESTION 288

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 291

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 296

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

- A. Transaction authentication

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

Answer: D

Explanation: Transaction authorization is the primary security concern for EDI environments.

NEW QUESTION 301

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

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

Answer: A

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

NEW QUESTION 304

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 306

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

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

Answer: D

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

NEW QUESTION 309

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 313

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 316

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

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

Answer: C

Explanation:

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

NEW QUESTION 319

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

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

Answer: A

Explanation:

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

NEW QUESTION 321

The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

- A. information assets are overprotecte
- B. a basic level of protection is applied regardless of asset valu
- C. appropriate levels of protection are applied to information asset
- D. an equal proportion of resources are devoted to protecting all information asset

Answer: C

Explanation:

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or underprotected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

NEW QUESTION 325

An organization's IS audit charter should specify the:

- A. short- and long-term plans for IS audit engagements
- B. objectives and scope of IS audit engagement
- C. detailed training plan for the IS audit staf
- D. role of the IS audit functio

Answer: D

Explanation:

An IS audit charter establishes the role of the information systems audit function. The charter should describe the overall authority, scope, and responsibilities of the audit function. It should be approved by the highest level of management and, if available, by the audit committee. Short-term and long-term planning is the responsibility of audit management. The objectives and scope of each IS audit should be agreed to in an engagement letter. A training plan, based on the audit plan, should be developed by audit management.

NEW QUESTION 330

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 333

In planning an audit, the MOST critical step is the identification of the:

- A. areas of high risk
- B. skill sets of the audit staff
- C. test steps in the audit
- D. time allotted for the audit

Answer: A

Explanation:

When designing an audit plan, it is important to identify the areas of highest risk to determine the areas to be audited. The skill sets of the audit staff should have been considered before deciding and selecting the audit. Test steps for the audit are not as critical as identifying the areas of risk, and the time allotted for an audit is determined by the areas to be audited, which are primarily selected based on the identification of risks.

NEW QUESTION 336

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

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

Answer: D

Explanation:

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

NEW QUESTION 341

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

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

Answer: A

Explanation:

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

NEW QUESTION 342

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

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

Answer: A

Explanation:

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

NEW QUESTION 343

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

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

Answer: D

Explanation:

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

NEW QUESTION 346

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

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

Answer: D

Explanation:

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

NEW QUESTION 351

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

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

Answer: A

Explanation:

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

NEW QUESTION 355

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- A. create the procedures document
- B. terminate the audit
- C. conduct compliance testing
- D. identify and evaluate existing practice

Answer: D

Explanation:

One of the main objectives of an audit is to identify potential risks; therefore, the most proactive approach would be to identify and evaluate the existing security practices being followed by the organization. IS auditors should not prepare documentation, as doing so could jeopardize their independence. Terminating the audit may prevent achieving one of the basic audit objectives, i.e., identification of potential risks. Since there are no documented procedures, there is no basis against which to test compliance.

NEW QUESTION 359

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

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

Answer: C

Explanation:

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

NEW QUESTION 362

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- A. test data to validate data input
- B. test data to determine system sort capabilities
- C. generalized audit software to search for address field duplication
- D. generalized audit software to search for account field duplication

Answer: C

Explanation:

Since the name is not the same (due to name variations), one method to detect duplications would be to compare other common fields, such as addresses. A subsequent review to determine common customer names at these addresses could then be conducted. Searching for duplicate account numbers would not likely find duplications, since customers would most likely have different account numbers for each variation. Test data would not be useful to detect the extent of any data characteristic, but simply to determine how the data were processed.

NEW QUESTION 364

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

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

Answer: D

Explanation:

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

NEW QUESTION 367

Data flow diagrams are used by IS auditors to:

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

Answer: C

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of data. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

NEW QUESTION 372

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 376

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

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

Answer: C

Explanation:

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

NEW QUESTION 377

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 382

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 386

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 388

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

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

Answer: A

Explanation:

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

NEW QUESTION 389

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

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

Answer: C

Explanation:

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

NEW QUESTION 394

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

- A. include the statement of management in the audit report
- B. identify whether such software is, indeed, being used by the organization
- C. reconfirm with management the usage of the software
- D. discuss the issue with senior management since reporting this could have a negative impact on the organization

Answer: B

Explanation:

When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

NEW QUESTION 395

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 396

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 399

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 404

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

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

Answer: C

Explanation:

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

NEW QUESTION 409

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

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

Answer: A

Explanation:

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

NEW QUESTION 414

Which of the following is the key benefit of control self-assessment (CSA)?

- A. Management ownership of the internal controls supporting business objectives is reinforced
- B. Audit expenses are reduced when the assessment results are an input to external audit work
- C. Improved fraud detection since internal business staff are engaged in testing controls
- D. Internal auditors can shift to a consultative approach by using the results of the assessment

Answer: A

Explanation:

The objective of control self-assessment is to have business management become more aware of the importance of internal control and their responsibility in terms of corporate governance. Reducing audit expenses is not a key benefit of control self-assessment (CSA). Improved fraud detection is important, but not as important as ownership, and is not a principal objective of CSA. CSA may give more insights to internal auditors, allowing them to take a more consultative role; however, this is an additional benefit, not the key benefit.

NEW QUESTION 418

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 420

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

- A. a lack of investment in technology
- B. a lack of a methodology for systems development
- C. technology not aligning with the organization's objective

D. an absence of control over technology contract

Answer: C

Explanation:

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

NEW QUESTION 423

An IS steering committee should:

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

Answer: C

Explanation:

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

NEW QUESTION 428

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

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

Answer: A

Explanation:

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

NEW QUESTION 433

IT governance is PRIMARILY the responsibility of the:

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

Answer: B

Explanation:

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

NEW QUESTION 438

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

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

Answer: A

Explanation:

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

NEW QUESTION 443

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

- A. Supplier and partner risks are manage
- B. A knowledge base on customers, products, markets and processes is in plac
- C. A structure is provided that facilitates the creation and sharing of business informatio
- D. Top management mediate between the imperatives of business and technolog

Answer: D

Explanation:

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

NEW QUESTION 445

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 447

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

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

Answer: C

Explanation:

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

NEW QUESTION 452

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

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

Answer: A

Explanation:

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

NEW QUESTION 455

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

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

Answer: B

Explanation:

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

NEW QUESTION 460

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

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

Answer: D

Explanation:

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

NEW QUESTION 462

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 on 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 464

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

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

Answer: C

Explanation:

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

NEW QUESTION 465

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 468

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

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

Answer: B

Explanation:

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

NEW QUESTION 472

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

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

Answer: A

Explanation:

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

NEW QUESTION 473

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

- A. Test a new accounting package
- B. Perform an evaluation of information technology needs
- C. Implement a new project planning system within the next 12 months
- D. Become the supplier of choice for the product offered

Answer: D

Explanation:

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

NEW QUESTION 475

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 trends

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 477

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

- A. has all the personnel and equipment it needs
- B. plans are consistent with management strategy
- C. uses its equipment and personnel efficiently and effectively
- D. has sufficient excess capacity to respond to changing directions

Answer: B

Explanation:

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

NEW QUESTION 480

In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

- A. Optimized
- B. Managed

- C. Defined
- D. Repeatable

Answer: B

Explanation:

Boards of directors and executive management can use the information security governance maturity model to establish rankings for security in their organizations. The ranks are nonexistent, initial, repeatable, defined, managed and optimized. When the responsibilities for IT security in an organization are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed, it is said to be 'managed and measurable.'

NEW QUESTION 482

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

- A. control self-assessment
- B. a business impact analysis
- C. an IT balanced scorecard
- D. business process reengineering

Answer: C

Explanation:

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

NEW QUESTION 486

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 487

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

- A. establishment of a review board
- B. creation of a security unit
- C. effective support of an executive sponsor
- D. selection of a security process owner

Answer: C

Explanation:

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

NEW QUESTION 488

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 489

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

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

Answer: A

Explanation:

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

NEW QUESTION 491

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CISA Practice Exam Features:

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