Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (Topic 1)
IS management has decided to rewrite a legacycustomer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

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

Answer: D

Explanation:

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

NEW QUESTION 2
- (Topic 1)
Which of the following 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 3
- (Topic 1)
Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

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

Answer: B

Explanation:

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

NEW QUESTION 4
- (Topic 1)
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 5
- (Topic 1)
Which of the following data validation edits is effective in detecting transposition and transcription errors?

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

Answer: B

Explanation:

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

NEW QUESTION 6
- (Topic 1)
A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

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

Answer: B

Explanation:

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

NEW QUESTION 7
- (Topic 1)
A data administrator is responsible for:

A. maintaining database system softwar
B. defining data elements, data names and their relationshi
C. developing physical database structure
D. developing data dictionary system softwar

Answer: B

Explanation:

A data administrator is responsible for defining data elements, data names and their relationship. Choices A, C and D are functions of a database administrator (DBA)

NEW QUESTION 8
- (Topic 1)
A database administrator is responsible for:

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

Answer: C

Explanation:

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

NEW QUESTION 9
- (Topic 1)
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 10
- (Topic 1)
A critical function of a firewall is to act as a:

A. special router that connects the Internet to a LA
B. device for preventing authorized users from accessing the LA
C. server used to connect authorized users to private trusted network resource
D. proxy server to increase the speed of access to authorized user

Answer: B

Explanation:

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users of other networks. An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling the outside resources to which its own users have access. Basically, a firewall, working closely with a router program, filters all network packets to determine whether or not to forward them toward their destination. A firewall includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so no incoming request can get directed to private network resources.

NEW QUESTION 10
- (Topic 1)
Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

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

Answer: D

Explanation:

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

NEW QUESTION 13
- (Topic 1)
Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

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

Answer: B

Explanation:

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

NEW QUESTION 14
- (Topic 1)
Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

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

Answer: A

Explanation:

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

NEW QUESTION 19
- (Topic 1)
For which of the following applications would rapid recovery be MOST crucial?

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

Answer: A

Explanation:

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

NEW QUESTION 22
- (Topic 1)
The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manua
B. performance of a comprehensive security control review by the IS audito
C. adoption of a corporate information security policy statemen
D. purchase of security access control softwar

Answer: C

Explanation:

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

NEW QUESTION 25
- (Topic 1)
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

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

Answer: C

Explanation:

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

NEW QUESTION 30
- (Topic 1)
How does the process of systems auditing benefit from using a risk-based approach to audit planning?

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

Answer: B

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

NEW QUESTION 32
- (Topic 1)
The use of statistical sampling procedures helps minimize:

A. Detection risk
B. Business risk
C. Controls risk
D. Compliance risk

Answer: A

Explanation:
The use of statistical sampling procedures helps minimize detection risk.

NEW QUESTION 34
- (Topic 1)
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

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

Answer: D

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

NEW QUESTION 39
- (Topic 1)
Who is ultimately accountable for the development of an IS security policy?

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

Answer: A

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

NEW QUESTION 42
- (Topic 1)
Batch control reconciliation is a _____________________ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

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

Answer: D

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

NEW QUESTION 46
- (Topic 1)
Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 47
- (Topic 1)
What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

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

Answer: B

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

NEW QUESTION 52
- (Topic 1)
An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

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

Answer: A

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

NEW QUESTION 54
- (Topic 1)
Why does the IS auditor often review the system logs?

A. To get evidence of password spoofing
B. To get evidence of data copy activities

C. To determine the existence of unauthorized access to data by a user or program
D. To get evidence of password sharing

Answer: C

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

NEW QUESTION 57
- (Topic 1)
What is essential for the IS auditor to obtain a clear understanding of network management?

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

Answer: C

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

NEW QUESTION 62
- (Topic 1)
What increases encryption overhead and cost the most?

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

Answer: B

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

NEW QUESTION 63
- (Topic 1)
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 65
- (Topic 1)
Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

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

Answer: C

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

NEW QUESTION 68
- (Topic 1)
Which of the following is a good control for protecting confidential data residing on a PC?

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

Answer: C

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

NEW QUESTION 70
- (Topic 1)
Which of the following do digital signatures provide?

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

Answer: A

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

NEW QUESTION 73
- (Topic 1)
Which of the following would provide the highest degree of server access control?

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

Answer: D

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

NEW QUESTION 77
- (Topic 1)
Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

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

Answer: A

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

NEW QUESTION 81
- (Topic 1)
Which of the following is an effective method for controlling downloading of files via FTP? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 85
- (Topic 1)
Which of the following provides the strongest authentication for physical access control?

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

Answer: D

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

NEW QUESTION 87
- (Topic 1)
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

A. OSI Layer 2 switches with packet filtering enabled

B. Virtual Private Networks
C. Access Control Lists (ACL)
D. Point-to-Point Tunneling Protocol

Answer: C

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

NEW QUESTION 90
- (Topic 1)
Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

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

Answer: A

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

NEW QUESTION 94
- (Topic 1)
Who is ultimately responsible and accountable for reviewing user access to systems?

A. Systems security administrators
B. Data custodians
C. Data owners
D. Information systems auditors

Answer: C

Explanation:
Data owners are ultimately responsible and accountable for reviewing user
access to systems.

NEW QUESTION 95
- (Topic 1)
Which of the following typically focuses on making alternative processes and resources available for transaction processing?

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

Answer: D

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

NEW QUESTION 99
- (Topic 1)
What influences decisions regarding criticality of assets?

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

Answer: C

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

NEW QUESTION 103
- (Topic 1)
With the objective of mitigating the risk and impact of a major business interruption, a disasterrecovery 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 106
- (Topic 1)
Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

A. Cold site
B. Hot site
C. Alternate site
D. Warm site

Answer: A

Explanation:
A cold site is often an acceptable solution for preparing for recovery of noncritical systems and datA.

NEW QUESTION 108
- (Topic 1)
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 111
- (Topic 1)
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive
management, such as the _______________. (fill-in-the-blank)

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

Answer: C

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

NEW QUESTION 115
- (Topic 1)
Library control software restricts source code to:

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

Answer: A

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

NEW QUESTION 116
- (Topic 1)
What is a primary high-level goal for an auditor who is reviewing a system development project?

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

Answer: C

Explanation:

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

NEW QUESTION 119
- (Topic 1)
Whenever an application is modified, what should be tested to determine the full impact of the change? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 120
- (Topic 1)
Who assumes ownership of a systems-development project and the resulting system?

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

Answer: A

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

NEW QUESTION 122
- (Topic 1)
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

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

Answer: B

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

NEW QUESTION 123
- (Topic 1)
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 127
- (Topic 1)
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

Answer: D

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

NEW QUESTION 128

- (Topic 1)
Run-to-run totals can verify data through which stage(s) of application processing?

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

Answer: B

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

NEW QUESTION 129
- (Topic 1)
________________ (fill in the blank) is/are are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 130
- (Topic 1)
Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 131
- (Topic 1)
What must an IS auditor understand before performing an application audit? Choose the BEST answer.

A. The potential business impact of application risk
B. Application risks must first be identifie
C. Relative business processe
D. Relevant application risk

Answer: C

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

NEW QUESTION 136
- (Topic 1)
What is the first step in a business process re-engineering project?

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

Answer: C

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

NEW QUESTION 138
- (Topic 1)
What is an edit check to determine whether a field contains valid data?

A. Completeness check
B. Accuracy check
C. Redundancy check
D. Reasonableness check

Answer: A

Explanation:
A completeness check is an edit check to determine whether a field contains valid datA.

NEW QUESTION 140
- (Topic 1)
Parity bits are a control used to validate:

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

Answer: B

Explanation:
Parity bits are a control used to validate data completeness.

NEW QUESTION 145
- (Topic 1)
The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

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

Answer: B

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

NEW QUESTION 147
- (Topic 1)
Which of the following is the MOST critical step in planning an audit?

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

Answer: C

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

NEW QUESTION 149
- (Topic 1)
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 153
- (Topic 1)
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Answer: D

Explanation:
When implementing continuous-monitoring systems, an IS auditor's first step is to identify highrisk areas within the organization.

NEW QUESTION 156
- (Topic 1)
What type of risk is associated with authorized program exits (trap doors)? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 159
- (Topic 1)
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Answer: A

Explanation:
It is true that an advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions.

NEW QUESTION 164
- (Topic 1)
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 managemen
B. To reassign job functions to eliminate potential frau
C. To implement compensator control
D. Segregation of duties is an administrative control not considered by an IS audito

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 167
- (Topic 1)
Why does an IS auditor review an organization chart?

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

Answer: C

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

NEW QUESTION 172
- (Topic 1)
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 176
- (Topic 1)
What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 177
- (Topic 1)
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 178
- (Topic 1)
Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 180
- (Topic 1)
What can be implemented to provide the highest level of protection from external attack?

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

Answer: A

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

NEW QUESTION 182
- (Topic 1)
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 183
- (Topic 1)
When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

A. The potential for unauthorized deletion of report copies
B. The potential for unauthorized modification of report copies
C. The potential for unauthorized printing of report copies
D. The potential for unauthorized editing of report copies

Answer: C

Explanation:
When reviewing print systems spooling, an IS auditor is most concerned with the potential for unauthorized printing of report copies.

NEW QUESTION 187
- (Topic 1)
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 189
- (Topic 1)
How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

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

Answer: A

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

NEW QUESTION 191
- (Topic 1)
Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

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

Answer: B

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

NEW QUESTION 196
- (Topic 1)
What are trojan horse programs? Choose the BEST answer.

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

Answer: D

Explanation:
Trojan horse programs are a common form of Internet attack.

NEW QUESTION 198
- (Topic 1)
What can be used to gather evidence of network attacks?

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

Answer: B

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

NEW QUESTION 203
- (Topic 1)
What is a callback system?

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

Answer: C

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

NEW QUESTION 205
- (Topic 1)
What type of fire-suppression system suppresses fire via water that is released from a main
valve to be delivered via a system of dry pipes installed throughout the facilities?

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

Answer: A

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

NEW QUESTION 208
- (Topic 1)
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

A. False
B. True

Answer: B

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

NEW QUESTION 209
- (Topic 1)
What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

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

Answer: C

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

NEW QUESTION 214
- (Topic 1)
What is often assured through table link verification and reference checks?

A. Database integrity
B. Database synchronization
C. Database normalcy
D. Database accuracy

Answer: A

Explanation:
Database integrity is most often ensured through table link verification and reference checks.

NEW QUESTION 216
- (Topic 1)
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 217
- (Topic 1)
Using the OSI reference model, what layer(s) is/are used to encrypt data?

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

Answer: C

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

NEW QUESTION 219
- (Topic 1)
When should systems administrators first assess the impact of applications or systems patches?

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

Answer: B

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

NEW QUESTION 224
- (Topic 1)
Rather than simply reviewing the adequacy of access control, appropriateness of access policies, and effectiveness of safeguards and procedures, the IS auditor is more concerned with effectiveness and utilization of assets. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 229
- (Topic 1)
The purpose of business continuity planning and disaster-recovery planning is to:

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

Answer: B

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

NEW QUESTION 232
- (Topic 1)
If a database is restored from information backed up before the last system image, which of the following is recommended?

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

Answer: B

Explanation:

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

NEW QUESTION 237
- (Topic 1)
An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 239
- (Topic 1)
Which of the following is the dominating objective of BCP and DRP?

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

Answer: A

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

NEW QUESTION 242
- (Topic 1)
Who is ultimately responsible for providing requirement specifications to the software-development team?

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

Answer: A

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

NEW QUESTION 247
- (Topic 1)
What should regression testing use to obtain accurate conclusions regarding the effects of changes or corrections to a program, and ensuring that those changes and corrections have not introduced new errors?

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

Answer: D

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

NEW QUESTION 249
- (Topic 1)
Which of the following processes are performed during the design phase of the systemsdevelopment life cycle (SDLC) model?

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

Answer: B

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

NEW QUESTION 251

- (Topic 1)
What is the most common reason for information systems to fail to meet the needs of users? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 252
- (Topic 1)
Who is responsible for the overall direction, costs, and timetables for systems-development projects?

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

Answer: B

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

NEW QUESTION 256
- (Topic 1)
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 261
- (Topic 1)
Input/output controls should be implemented for which applications in an integrated systems environment?

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

Answer: C

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

NEW QUESTION 265
- (Topic 1)
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

A. Before transaction completion
B. Immediately after an EFT is initiated
C. During run-to-run total testing
D. Before an EFT is initiated

Answer: D

Explanation:
An application-level edit check to verify availability of funds should be completed at the electronic funds transfer (EFT) interface before an EFT is initiated.

NEW QUESTION 268
- (Topic 1)
_________________ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

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

Answer: A

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

NEW QUESTION 269
- (Topic 1)
Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 270
- (Topic 1)
What is a data validation edit control that matches input data to an occurrence rate? Choose the BEST answer.

A. Accuracy check
B. Completeness check
C. Reasonableness check
D. Redundancy check

Answer: C

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

NEW QUESTION 274
- (Topic 1)
Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 275
- (Topic 1)
An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

A. Substantive
B. Compliance
C. Integrated
D. Continuous audit

Answer: A

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

NEW QUESTION 279
- (Topic 2)
An IS auditor is reviewing access to an application to determine whether the 10 most recent "new user" forms were correctly authorized. This is an example of:

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

Answer: C

Explanation:

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

NEW QUESTION 283
- (Topic 2)
The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

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

Answer: B

Explanation:

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

NEW QUESTION 284
- (Topic 2)
Which of the following is a substantive test?

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

Answer: C

Explanation:

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

NEW QUESTION 289
- (Topic 2)
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 290
- (Topic 2)
Which of the following sampling methods is MOST useful when testing for compliance?

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

Answer: A

Explanation:

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

NEW QUESTION 291
- (Topic 2)
The PRIMARY purpose of audit trails is to:

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

Answer: B

Explanation:

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

NEW QUESTION 293
- (Topic 2)
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

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

Answer: C

Explanation:

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

NEW QUESTION 296
- (Topic 2)
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 297
- (Topic 2)
An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

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

Answer: D

Explanation:

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

NEW QUESTION 299
- (Topic 2)
The extent to which data will be collected during an IS audit should be determined based on the:

A. availability of critical and required informatio
B. auditor's familiarity with the circumstance
C. auditee's ability to find relevant evidenc
D. purpose and scope of the audit being don

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 thescope of the audit should not be limited by the auditee's ability to find relevant evidence.

NEW QUESTION 303
- (Topic 2)
During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

A. address audit objective
B. collect sufficient evidenc
C. specify appropriate test
D. minimize audit resource

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 theyare 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 305
- (Topic 2)
An IS auditor evaluating logical access controls should FIRST:

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

Answer: D

Explanation:

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

NEW QUESTION 310
- (Topic 2)
The PRIMARY purpose of an IT forensic audit is:

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

Answer: B

Explanation:

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

NEW QUESTION 313
- (Topic 2)
An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

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

Answer: D

Explanation:

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

NEW QUESTION 316
- (Topic 2)
An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

A. matching control totals of the imported data to control totals of the original dat

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

Answer: A

Explanation:

Matching control totals of the imported data with control totals of the original data is the next logical step, as this confirms the completeness of the imported datA. It is not possible to confirm completeness by sorting the imported data, because the original data may not be in sorted order. Further, sorting does not provide control totals for verifying completeness. Reviewing a printout of 100 records of original data with 100 records of imported data is a process of physical verification andconfirms 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 320
- (Topic 2)
Which of the following would normally be the MOST reliable evidence for an auditor?

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

Answer: A

Explanation:

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

NEW QUESTION 321
- (Topic 2)
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 inpu
B. test data to determine system sort capabilitie
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 326
- (Topic 2)
Which of the following would be the BEST population to take a sample from when testing program changes?

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

Answer: D

Explanation:

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

NEW QUESTION 328
- (Topic 2)
An integrated test facility is considered a useful audit tool because it:

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

Answer: C

Explanation:

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

NEW QUESTION 329
- (Topic 2)
Data flow diagrams are used by IS auditors to:

A. order data hierarchicall
B. highlight high-level data definition
C. graphically summarize data paths and storag
D. portray step-by-step details of data generatio

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 334
- (Topic 2)
An IS auditor reviews an organizational chart PRIMARILY for:

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

Answer: C

Explanation:

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

NEW QUESTION 335
- (Topic 2)
Which of the following is an advantage of an integrated test facility (ITF)?

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

Answer: B

Explanation:

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

NEW QUESTION 340
- (Topic 2)
When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

A. topology diagram
B. bandwidth usag
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 342
- (Topic 2)
While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

A. Observe the response mechanis
B. Clear the virus from the networ
C. Inform appropriate personnel immediatel
D. Ensure deletion of the viru

Answer: C

Explanation:

The first thing an IS auditor should do after detecting the virus is to alert the organization to its presence, then wait for their response. Choice A should be taken after choice C. This will enable an IS auditor to examine the actual workability and effectiveness of the response system. An IS auditor should not make changes to the system being audited, and ensuring the deletion of the virus is a management responsibility.

NEW QUESTION 347
- (Topic 2)
An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

A. conclude that the controls are inadequat
B. expand the scope to include substantive testin
C. place greater reliance on previous audit
D. suspend the audi

Answer: B

Explanation:

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

NEW QUESTION 352
- (Topic 2)
In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

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

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 356
- (Topic 2)
Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

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

Answer: C

Explanation:

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

NEW QUESTION 361
- (Topic 2)
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 repor
B. identify whether such software is, indeed, being used by the organizatio
C. reconfirm with management the usage of the softwar
D. discuss the issue with senior management since reporting this could have a negative impact on the organizatio

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 365
- (Topic 2)
The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

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

Answer: B

Explanation:

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

NEW QUESTION 367
- (Topic 2)
During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

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

Answer: C

Explanation:

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

NEW QUESTION 368
- (Topic 2)
An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 373
- (Topic 2)
Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

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

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 378
- (Topic 2)

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not beingchecked properly. While preparing the audit report, the IS auditor should:

A. record the observations separately with the impact of each of them marked against each respective findin
B. advise the manager of probable risks without recording the observations, as the control weaknesses are minor one
C. record the observations and the risk arising from the collective weaknesse
D. apprise the departmental heads concerned with each observation and properly document it in the repor

Answer: C

Explanation:

Individually the weaknesses are minor; however, together they have the potential to substantially weaken the overall control structure. Choices A and D reflect a failure on the part of an IS auditor to recognize the combined affect of the control weakness. Advising the local manager without reporting the facts and observations would conceal the findings from other stakeholders.

NEW QUESTION 383
- (Topic 2)
During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

A. ask the auditee to sign a release form accepting full legal responsibilit
B. elaborate on the significance of the finding and the risks of not correcting i
C. report the disagreement to the audit committee for resolutio
D. accept the auditee's position since they are the process owner

Answer: B

Explanation:

If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposures, as the auditee may not fully appreciate the magnitude of the exposure. The goal should be to enlighten the auditee or uncover new information of which an IS auditor may not have been aware. Anything that appears to threaten the auditee will lessen effective communications and set up an adversarial relationship. By the same token, an IS auditor should not automatically agree just because the auditee expresses an alternate point of view.

NEW QUESTION 384
- (Topic 2)
When preparing an audit report the IS auditor should ensure that the results are supported by:

A. statements from IS managemen
B. workpapers of other auditor
C. an organizational control self-assessmen
D. sufficient and appropriate audit evidenc

Answer: D

Explanation:

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

NEW QUESTION 388
- (Topic 2)
The final decision to include a material finding in an audit report should be made by the:

A. audit committe
B. auditee's manage
C. IS audito
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 392
- (Topic 2)
A PRIMARY benefit derived from an organization employing control self-assessment (CSA) techniques is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 395
- (Topic 2)
Which of the following is an attribute of the control self-assessment (CSA) approach?

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

Answer: A

Explanation:

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

NEW QUESTION 397
- (Topic 3)
An IT steering committee should review information systems PRIMARILY to assess:

A. whether IT processes support business requirement
B. if proposed system functionality is adequat
C. the stability of existing softwar
D. the complexity of installed technolog

Answer: A

Explanation:

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

NEW QUESTION 400
- (Topic 3)
The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technolog
B. a lack of a methodology for systems developmen
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 404
- (Topic 3)
Involvement of senior management is MOST important in the development of:

A. strategic plan
B. IS policie
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 408
- (Topic 3)
IT governance is PRIMARILY the responsibility of the:

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

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 412
- (Topic 3)
As an outcome of information security governance, strategic alignment provides:

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

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 413
- (Topic 3)
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 andprocesses 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 418
- (Topic 3)
The ultimate purpose of IT governance is to:

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

Answer: A

Explanation:

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

NEW QUESTION 420
- (Topic 3)
What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

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

Answer: B

Explanation:

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

NEW QUESTION 423
- (Topic 3)
Responsibility for the governance of IT should rest with the:

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

Answer: D

Explanation:

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

NEW QUESTION 428
- (Topic 3)
Which of the following would BEST provide assurance of the integrity of new staff?

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

Answer: A

Explanation:

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

NEW QUESTION 430
- (Topic 3)
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual'sexperience and:

A. length of service, since this will help ensure technical competenc
B. age, as training in audit techniques may be impractica
C. IS knowledge, since this will bring enhanced credibility to the audit functio
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 435
- (Topic 3)
An IS auditor should be concerned when a telecommunication analyst:

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

Answer: A

Explanation:

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes {choice B), assessing the impact of network load or terminal response times and network data transferrates (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 436
- (Topic 3)
Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

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

Answer: D

Explanation:

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

NEW QUESTION 438
- (Topic 3)
Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

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

Answer: A

Explanation:

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

NEW QUESTION 442
- (Topic 3)
Which of the following is normally a responsibility of the chief security officer (CSO)?

A. Periodically reviewing and evaluating the security policy
B. Executing user application and software testing and evaluation
C. Granting and revoking user access to IT resources
D. Approving access to data and applications

Answer: A

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

NEW QUESTION 447
- (Topic 3)
Which of the following goals would you expect to find in an organization's strategic plan?

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

Answer: D

Explanation:

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

NEW QUESTION 452
- (Topic 3)
An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environmen
B. the business pla

C. the present IT budge
D. current technology trend

Answer: B

Explanation:

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

NEW QUESTION 453
- (Topic 3)
When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

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

Answer: B

Explanation:

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

NEW QUESTION 454
- (Topic 3)
To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

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

Answer: C

Explanation:

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

NEW QUESTION 458
- (Topic 3)
When reviewing the IT strategic planning process, an IS auditor should ensure that the plan:

A. incorporates state of the art technolog
B. addresses the required operational control
C. articulates the IT mission and visio
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 461
- (Topic 3)
When developing a formal enterprise security program, the MOST critical success factor (CSF) would be the:

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

Answer: C

Explanation:

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

NEW QUESTION 466

- (Topic 3)
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

A. User management coordination does not exis
B. Specific user accountability cannot be establishe
C. Unauthorized users may have access to originate, modify or delete dat
D. Audit recommendations may not be implemente

Answer: C

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

NEW QUESTION 469
- (Topic 3)
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

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

Answer: A

Explanation:

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

NEW QUESTION 470
- (Topic 3)
A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

A. recover
B. retentio
C. rebuildin
D. reus

Answer: B

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the officialform of classic 'paper* makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

NEW QUESTION 473
- (Topic 3)
A top-down approach to the development of operational policies will help ensure:

A. that they are consistent across the organizatio
B. that they are implemented as a part of risk assessmen
C. compliance with all policie
D. that they are reviewed periodicall

Answer: A

Explanation:

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

NEW QUESTION 474
- (Topic 3)
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

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

Answer: C

Explanation:

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

NEW QUESTION 479
- (Topic 3)
A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

A. Issues of privacy
B. Wavelength can be absorbed by the human body
C. RFID tags may not be removable
D. RFID eliminates line-of-sight reading

Answer: A

Explanation:

The purchaser of an item will not necessarily be aware of the presence of the tag. If a tagged item is paid for by credit card, it would be possible to tie the unique ID of that item to the identity of the purchaser. Privacy violations are a significant concern because RFID can carry unique identifier numbers. If desired it would be possible for a firm to track individuals who purchase an item containing an RFID. Choices B and C are concerns of less importance. Choice D is not a concern.

NEW QUESTION 481
- (Topic 3)
When developing a security architecture, which of the following steps should be executed FIRST?

A. Developing security procedures
B. Defining a security policy
C. Specifying an access control methodology
D. Defining roles and responsibilities

Answer: B

Explanation:

Defining a security policy for information and related technology is the first step toward building a security architecture. A security policy communicates a coherent security standard to users, management and technical staff. Security policies willoften set the stage in terms of what tools and procedures are needed for an organization. The other choices should be executed only after defining a security policy.

NEW QUESTION 485
- (Topic 3)
The initial step in establishing an information security program is the:

A. development and implementation of an information security standards manua
B. performance of a comprehensive security control review by the IS audito
C. adoption of a corporate information security policy statemen
D. purchase of security access control softwar

Answer: C

Explanation:

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

NEW QUESTION 486
- (Topic 3)
The PRIMARY objective of implementing corporate governance by an organization's management is to:

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

Answer: A

Explanation:

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

NEW QUESTION 490
- (Topic 3)
Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

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

Answer: C

Explanation:

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

NEW QUESTION 494
- (Topic 3)
An example of a direct benefit to be derived from a proposed IT-related business investment is:

A. enhanced reputatio
B. enhanced staff moral
C. the use of new technolog
D. increased market penetratio

Answer: D

Explanation:

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

NEW QUESTION 497
- (Topic 3)
A benefit of open system architecture is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 501
- (Topic 3)
After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

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

Answer: B

Explanation:

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

NEW QUESTION 506
- (Topic 3)
Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees

D. Monitoring the outsourcing provider's performance

Answer: D

Explanation:

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

NEW QUESTION 509
- (Topic 3)
An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

A. hardware configuratio
B. access control softwar
C. ownership of intellectual propert
D. application development methodolog

Answer: C

Explanation:

Of the choices, the hardware and access control software is generally irrelevant as long as the functionality, availability and security can be affected, which are specific contractual obligations. Similarly, the development methodology should be ofno real concern. The contract must, however, specify who owns the intellectual property (i.e., information being processed, application programs). Ownership of intellectual property will have a significant cost and is a key aspect to be defined in an outsourcing contract.

NEW QUESTION 511
- (Topic 3)
To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

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

Answer: B

Explanation:

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

NEW QUESTION 512
- (Topic 3)
When an organization is outsourcing their information security function, which of the following should be kept in the organization?

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

Answer: A

Explanation:

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

NEW QUESTION 513
......

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

* CISA Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CISA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The CISA Practice Test Here