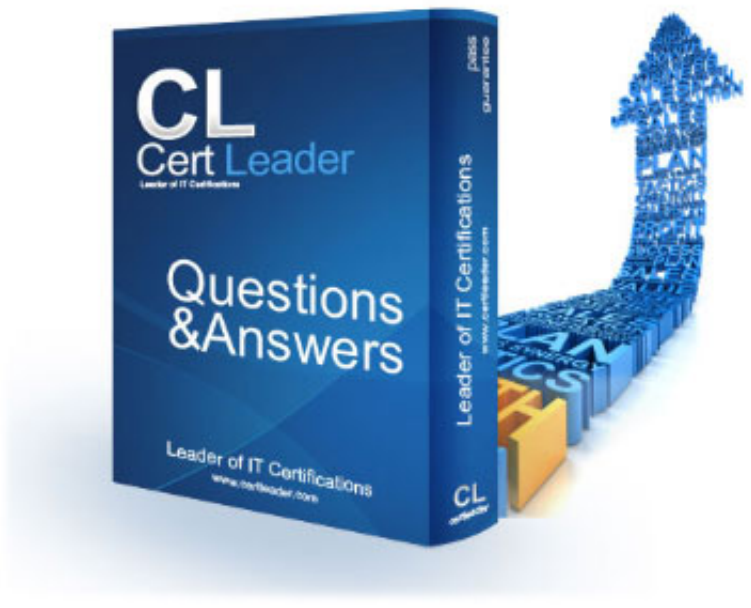
CISA Dumps

Isaca CISA

https://www.certleader.com/CISA-dumps.html



NEW QUESTION 1
- (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 2
- (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 3
- (Topic 1)
An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

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

Answer: A

Explanation:

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

NEW QUESTION 4
- (Topic 1)
Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

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

Answer: C

Explanation:

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

NEW QUESTION 5
- (Topic 1)
To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

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

Answer: A

Explanation:

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

NEW QUESTION 6
- (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 7
- (Topic 1)
A LAN administrator normally would be restricted from:

A. having end-user responsibilitie
B. reporting to the end-user manage
C. having programming responsibilitie
D. being responsible for LAN security administratio

Answer: C

Explanation:

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

NEW QUESTION 8
- (Topic 1)
For which of the following applications would rapid recovery be MOST crucial?

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

Answer: A

Explanation:

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

NEW QUESTION 9
- (Topic 1)
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 10
- (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 10
- (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 15
- (Topic 1)
If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

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

Answer: C

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

NEW QUESTION 16
- (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 17
- (Topic 1)
How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

A. EDI usually decreases the time necessary for revie
B. EDI usually increases the time necessary for revie
C. Cannot be determine
D. EDI does not affect the time necessary for revie

Answer: A

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

NEW QUESTION 19
- (Topic 1)
What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

A. Network-monitoring software
B. A system downtime log
C. Administration activity reports
D. Help-desk utilization trend reports

Answer: B

Explanation:
A system downtime log can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program.

NEW QUESTION 21
- (Topic 1)
What are used as a countermeasure for potential database corruption when two processes attempt to simultaneously edit or update the same information? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 22
- (Topic 1)
Which of the following best characterizes "worms"?

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

Answer: A

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

NEW QUESTION 25
- (Topic 1)
Regarding digital signature implementation, which of the following answers is correct?

A. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private ke
B. Upon receiving the data, the recipient can decrypt the data using the sender's public ke
C. A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public ke
D. Upon receiving the data, the recipient can decrypt the data using the recipient's public ke
E. A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message content
F. Upon receiving the data, the recipient can independently create i
G. A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public ke
H. Upon receiving the data, the recipient can decrypt the data using the recipient's private ke

Answer: C

Explanation:
A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value, or message digest, from the entire message contents. Upon receiving the data, the recipient can independently create its own message digest from the data for comparison and data integrity validation. Public and private are used to enforce confidentiality. Hashing algorithms are used to enforce integrity.

NEW QUESTION 27
- (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 28
- (Topic 1)
What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off? Choose the BEST answer.

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

Answer: C

Explanation:
Screensaver passwords are an effective control to implement as a countermeasure for the vulnerability of data entry operators potentially leaving their computers

without logging off.

NEW QUESTION 33
- (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 35
- (Topic 1)
Which of the following is used to evaluate biometric access controls?

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

Answer: B

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

NEW QUESTION 38
- (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 39
- (Topic 1)
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

A. End-user involvement
B. Senior management involvement
C. Security administration involvement
D. IS auditing involvement

Answer: A

Explanation:
End-user involvement is critical during the business impact assessment phase of business continuity planning.

NEW QUESTION 42
- (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 45
- (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 49
- (Topic 1)
Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 52
- (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 55
- (Topic 1)
The quality of the metadata produced from a data warehouse is _____ in the warehouse's design. Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 57
- (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 62
- (Topic 1)
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 67
- (Topic 1)
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

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

Answer: A

Explanation:
A redundancy check can help detect transmission errors by appending especially calculated bits onto the end of each segment of datA.

NEW QUESTION 71
- (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 74
- (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 76
- (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 78
- (Topic 1)
An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated datA. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 80
- (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 83
- (Topic 1)
Ensuring that security and control policies support business and IT objectives is a primary objective of:

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

Answer: A

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

NEW QUESTION 86
- (Topic 1)
When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

A. Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic pla
B. Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic pla
C. Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic pla
D. Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic pla

Answer: A

Explanation:
Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.

NEW QUESTION 87
- (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 89
- (Topic 1)
What supports data transmission through split cable facilities or duplicate cable facilities?

A. Diverse routing
B. Dual routing
C. Alternate routing
D. Redundant routing

Answer: A

Explanation:
Diverse routing supports data transmission through split cable facilities, or duplicate cable facilities.

NEW QUESTION 94
- (Topic 1)
What is a common vulnerability, allowing denial-of-service attacks?

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

D. Configuring firewall access rules

Answer: C

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

NEW QUESTION 96
- (Topic 1)
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

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

Answer: C

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

NEW QUESTION 101
- (Topic 1)
What process is used to validate a subject's identity?

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

Answer: D

Explanation:
Authentication is used to validate a subject's identity.

NEW QUESTION 105
- (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 110
- (Topic 1)
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 111
- (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 113
- (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 114
- (Topic 1)
Which of the following is of greatest concern when performing an IS audit?

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

Answer: A

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

NEW QUESTION 118
- (Topic 1)
What are intrusion-detection systems (IDS) primarily used for?

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

Answer: D

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

NEW QUESTION 120
- (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 125
- (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 129
- (Topic 1)
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

A. By implementing redundant systems and applications onsite
B. By geographically dispersing resources
C. By retaining onsite data backup in fireproof vaults
D. By preparing BCP and DRP documents for commonly identified disasters

Answer: B

Explanation:
Minimizing single points of failure or vulnerabilities of a common disaster is mitigated by geographically dispersing resources.

NEW QUESTION 131
- (Topic 1)
Off-site data storage should be kept synchronized when preparing for recovery of time-sensitive data such as that resulting from which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 132
- (Topic 1)
Why is a clause for requiring source code escrow in an application vendor agreement important?

A. To segregate systems development and live environments
B. To protect the organization from copyright disputes
C. To ensure that sufficient code is available when needed
D. To ensure that the source code remains available even if the application vendor goes out of business

Answer: D

Explanation:
A clause for requiring source code escrow in an application vendor agreement is important to ensure that the source code remains available even if the application vendor goes out of business.

NEW QUESTION 136
- (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 141
- (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 143
- (Topic 1)
When should application controls be considered within the system-development process?

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

Answer: D

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

specifications.

NEW QUESTION 148
- (Topic 1)
What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

A. Rapid application development (RAD)
B. GANTT
C. PERT
D. Decision trees

Answer: A

Explanation:
Rapid application development (RAD) is used to develop strategically important systems faster, reduce development costs, and still maintain high quality.

NEW QUESTION 151
- (Topic 1)
What is the primary security concern for EDI environments? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 152
- (Topic 1)
Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 154
- (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 159
- (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 164
- (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 169
- (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 170
- (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 172
- (Topic 2)
An audit charter should:

A. be dynamic and change often to coincide with the changing nature of technology and the audit professio
B. clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal control
C. document the audit procedures designed to achieve the planned audit objective
D. outline the overall authority, scope and responsibilities of the audit functio

Answer: D

Explanation:
An audit charter should state management's objectives for and delegation of authority to IS audit. This charter should not significantly change over time and should be approved at the highest level of management. An audit charter would not be at a detailed level and, therefore, would not include specific audit objectives or procedures.

NEW QUESTION 173
- (Topic 2)
The PRIMARY advantage of a continuous audit approach is that it:

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

Answer: C

Explanation:

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

NEW QUESTION 176
- (Topic 2)

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

A. controls needed to mitigate risks are in plac
B. vulnerabilities and threats are identifie
C. audit risks are considere
D. a gap analysis is appropriat

Answer: B

Explanation:

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

NEW QUESTION 180
- (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 185
- (Topic 2)
In planning an audit, the MOST critical step is the identification of the:

A. areas of high ris
B. skill sets of the audit staf
C. test steps in the audi
D. time allotted for the audi

Answer: A

Explanation:

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

NEW QUESTION 189
- (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 191
- (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 193
- (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, theIS 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 195
CORRECT TEXT - (Topic 2)
The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

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

Answer: B

NEW QUESTION 196
- (Topic 2)
In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 197
- (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 201
- (Topic 2)
An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

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

Answer: B

Explanation:

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

NEW QUESTION 202
- (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 206
- (Topic 2)
When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

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

Answer: C

Explanation:

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

NEW QUESTION 208
- (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 210
- (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 212
- (Topic 2)
During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

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

Answer: B

Explanation:

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

NEW QUESTION 217
- (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 219
- (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 221
- (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 224
- (Topic 2)
Which of the following is the key benefit of control self-assessment (CSA)?

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

Answer:

A

Explanation:

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

NEW QUESTION 227
- (Topic 3)
Which of the following is a function of an IS steering committee?

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

Answer: C

Explanation:

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

NEW QUESTION 231
- (Topic 3)
Establishing the level of acceptable risk is the responsibility of:

A. quality assurance managemen
B. senior business managemen
C. the chief information office
D. the chief security office

Answer: B

Explanation:

Senior management should establish the acceptable risk level, since they have the ultimate or final responsibility for the effective and efficient operation of the organization. Choices A, C and D should act as advisors to senior management in determining an acceptable risk level.

NEW QUESTION 235
- (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 236
- (Topic 3)
Which of the following is the MOST important element for the successful implementation of IT governance?

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

Answer: B

Explanation:

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

NEW QUESTION 240

- (Topic 3)
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

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

Answer: C

Explanation:

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

NEW QUESTION 241
- (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 244
- (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 245
- (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 249
- (Topic 3)
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protectio
B. Job descriptions contain clear statements of accountability for information securit

C. In accordance with the degree of risk and business impact, there is adequate funding for security effort
D. No actual incidents have occurred that have caused a loss or a public embarrassmen

Answer: B

Explanation:

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

NEW QUESTION 253
- (Topic 3)
To support an organization's goals, an IS department should have:

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

Answer: B

Explanation:

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

NEW QUESTION 256
- (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 259
- (Topic 3)
In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

A. Optimized
B. Managed
C. Defined
D. Repeatable

Answer: B

Explanation:

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

NEW QUESTION 261
- (Topic 3)
The development of an IS security policy is ultimately the responsibility of the:

A. IS departmen
B. security committe
C. security administrato
D. board of director

Answer: D

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed

by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

NEW QUESTION 263
- (Topic 3)
Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

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

Answer: A

Explanation:

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

NEW QUESTION 266
- (Topic 3)
Which of the following is the initial step in creating a firewall policy?

A. A cost-benefit analysis of methods for securing the applications
B. Identification of network applications to be externally accessed
C. Identification of vulnerabilities associated with network applications to be externally accessed
D. Creation of an applications traffic matrix showing protection methods

Answer: B

Explanation:

Identification of the applications required across the network should be identified first. After identification, depending on the physical location of these applications in the network and the network model, the person in charge will be able to understand the need for, and possible methods of, controlling access to these applications. Identifying methods to protect against identified vulnerabilities and their comparative cost-benefit analysis is the third step. Having identified the applications, the next step is to identify vulnerabilities (weaknesses) associated with the network applications. The next step is to analyze the application traffic and create a matrix showing how each type of traffic will be protected.

NEW QUESTION 267
- (Topic 3)
The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

A. Utilization of an intrusion detection system to report incidents
B. Mandating the use of passwords to access all software
C. Installing an efficient user log system to track the actions of each user
D. Training provided on a regular basis to all current and new employees

Answer: D

Explanation:

Utilizing an intrusion detection system to report on incidents that occur is an implementation of a security program and is not effective in establishing a security awareness program. Choices B and C do not address awareness. Training is the only choice that is directed at security awareness.

NEW QUESTION 271
- (Topic 3)
To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

A. the IT infrastructur
B. organizational policies, standards and procedure
C. legal and regulatory requirement
D. the adherence to organizational policies, standards and procedure

Answer: C

Explanation:

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

NEW QUESTION 276
- (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 279
- (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 282
- (Topic 3)
Which of the following provides the best evidence of the adequacy of a security awareness program?

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

Answer: D

Explanation:

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

NEW QUESTION 285
- (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 289
- (Topic 3)
To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

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

Answer: D

Explanation:

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

NEW QUESTION 290
- (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 291
- (Topic 3)
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

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

Answer: A

Explanation:

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

NEW QUESTION 292
- (Topic 3)
With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

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

Answer: A

Explanation:

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

NEW QUESTION 297
- (Topic 3)
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern shouldbe that the:

A. requirement for protecting confidentiality of information could be compromise
B. contract may be terminated because prior permission from the outsourcer was not obtaine
C. other service provider to whom work has been outsourced is not subject to audi
D. outsourcer will approach the other service provider directly for further wor

Answer: A

Explanation:

Many countries have enacted regulations to protect the confidentiality of information maintained in their countries and/or exchanged with other countries. Where a service provider outsources part of its services to another service provider, there is a potential risk that the confidentiality of the information will be compromised. Choices B and C could be concerns but are not related to ensuring the confidentiality of information. There is no reason why an IS auditor should be concerned with choice D.

NEW QUESTION 298
- (Topic 3)
An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement (SLA) between the organization and vendor should be the provisions for:

A. documentation of staff background check
B. independent audit reports or full audit acces
C. reporting the year-to-year incremental cost reduction
D. reporting staff turnover, development or trainin

Answer: B

Explanation:

When the functions of an IS department are outsourced, an IS auditor should ensure that a provision is made for independent audit reports that cover all essential areas, or that the outsourcer has full audit access. Although it is necessary to document the fact that background checks are performed, this is not as important as provisions for audits. Financial measures such as year-to-year incremental cost reductions are desirable to have in a service level agreement (SLA); however, cost reductions are not as important as the availability of independent audit reports or full audit access. An SLA might include human relationship measures such as resource planning, staff turnover, development or training, but this is not as important as the requirements for independent reports or full audit access by the outsourcing organization.

NEW QUESTION 301
- (Topic 3)
The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

A. destruction polic
B. security polic
C. archive polic
D. audit polic

Answer: C

Explanation:

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

NEW QUESTION 305
- (Topic 3)
An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

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

Answer: C

Explanation:

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

NEW QUESTION 309
- (Topic 3)
Assessing IT risks is BEST achieved by:

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

Answer: A

Explanation:

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

NEW QUESTION 310
- (Topic 3)
To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

A. avoidanc
B. transferenc
C. mitigatio
D. acceptanc

Answer: C

Explanation:

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

NEW QUESTION 315
- (Topic 3)
An IS auditor reviewing the risk assessment process of an organization should FIRST:

A. identify the reasonable threats to the information asset
B. analyze the technical and organizational vulnerabilitie
C. identify and rank the information asset
D. evaluate the effect of a potential security breac

Answer: C

Explanation:

Identification and ranking of information assets-e.g., data criticality, locations of assets-will set the tone or scope of how to assess risk in relation to the organizational value of the asset. Second, the threats facing each of the organization's assets should be analyzed according to their value to the organization. Third, weaknesses should be identified so that controls can be evaluated to determine if they mitigate the weaknesses. Fourth, analyze how these weaknesses, in absence of given controls, would impact the organization information assets.

NEW QUESTION 317
- (Topic 3)
As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

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

Answer: A

Explanation:

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

NEW QUESTION 322
- (Topic 3)
The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

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

Answer: B

Explanation:

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

NEW QUESTION 325
- (Topic 3)
An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

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

Answer: A

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the

past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

NEW QUESTION 327
- (Topic 4)
Documentation of a business case used in an IT development project should be retained until:

A. the end of the system's life cycl
B. the project is approve
C. user acceptance of the syste
D. the system is in productio

Answer: A

Explanation:

A business case can and should be used throughout the life cycle of the product. It serves as an anchor for new (management) personnel, helps to maintain focus and provides valuable information on estimates vs. actuals. Questions like, 'why dowe do that,"what was the original intent' and 'how did we perform against the plan' can be answered, and lessons for developing future business cases can be learned. During the development phase of a project one shouldalways validate the business case, as it is a good management instrument. After finishing a project and entering production, the business case and all the completed research are valuable sources of information that should be kept for further reference

NEW QUESTION 328
- (Topic 4)
Which of the following is a characteristic of timebox management?

A. Not suitable for prototyping or rapid application development (RAD)
B. Eliminates the need for a quality process
C. Prevents cost overruns and delivery delays
D. Separates system and user acceptance testing

Answer: C

Explanation:

Timebox management, by its nature, sets specific time and cost boundaries. It is very suitable for prototyping and RAD, and integrates system and user acceptance testing, but does not eliminate the need for a quality process.

NEW QUESTION 331
- (Topic 4)
An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

A. complexity and risks associated with the project have been analyze
B. resources needed throughout the project have been determine
C. project deliverables have been identifie
D. a contract for external parties involved in the project has been complete

Answer: A

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

NEW QUESTION 336
- (Topic 4)
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

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

Answer: A

Explanation:

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

NEW QUESTION 339
- (Topic 4)
Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

A. Function point analysis
B. Earned value analysis
C. Cost budget
D. Program Evaluation and Review Technique

Answer: B

Explanation:

Earned value analysis (EVA) is an industry standard method for measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds. It compares the planned amount of work with what has actually been completed, to determine if the cost, schedule and work accomplished are progressing in accordance with the plan. EVA works most effectively if a well-formed work breakdown structure exists. Function point analysis (FPA) is an indirect measure of software size and complexity and, therefore, does not address the elements of time and budget. Cost budgets do not address time. PERT aids in time and deliverables management, but lacks projections for estimates at completion (EACs) and overall financial management.

NEW QUESTION 341
- (Topic 4)
When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

A. project be discontinue
B. business case be updated and possible corrective actions be identifie
C. project be returned to the project sponsor for reapprova
D. project be completed and the business case be updated late

Answer: B

Explanation:

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

NEW QUESTION 342
- (Topic 4)
Which of the following situations would increase the likelihood of fraud?

A. Application programmers are implementing changes to production program
B. Application programmers are implementing changes to test program
C. Operations support staff are implementing changes to batch schedule
D. Database administrators are implementing changes to data structure

Answer: A

Explanation:

Production programs are used for processing an enterprise's datA. It is imperative that controls on changes to production programs are stringent. Lack of control in this area could result in application programs being modified to manipulate the data.Application programmers are required to implement changes to test programs. These are used only in development and do not directly impact the live processing of datA. The implementation of changes to batch schedules by operations support staff willaffect the scheduling of the batches only; it does not impact the live datA. Database administrators are required to implement changes to data structures. This is required for reorganization of the database to allow for additions, modifications or deletions of fields or tables in the database.

NEW QUESTION 344
- (Topic 4)
The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

A. integrit
B. authenticit
C. authorizatio
D. nonrepudiatio

Answer: A

Explanation:

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

NEW QUESTION 348
- (Topic 4)
The editing/validation of data entered at a remote site would be performed MOST effectively at the:

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

Answer: D

Explanation:

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

NEW QUESTION 349
- (Topic 4)
To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

A. during data preparatio
B. in transit to the compute
C. between related computer run
D. during the return of the data to the user departmen

Answer: A

Explanation:

During data preparation is the best answer, because it establishes control at the earliest point.

NEW QUESTION 353
- (Topic 4)
What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

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

Answer: B

Explanation:

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

NEW QUESTION 355
- (Topic 4)
Which of the following is the GREATEST risk to the effectiveness of application system controls?

A. Removal of manual processing steps
B. inadequate procedure manuals
C. Collusion between employees
D. Unresolved regulatory compliance issues

Answer: C

Explanation:

Collusion is an active attack that can be sustained and is difficult to identify since even well-thought-out application controls may be circumvented. The other choices do not impact well-designed application controls.

NEW QUESTION 358
- (Topic 4)
The MAIN purpose of a transaction audit trail is to:

A. reduce the use of storage medi
B. determine accountability and responsibility for processed transaction
C. help an IS auditor trace transaction
D. provide useful information for capacity plannin

Answer: B

Explanation:

Enabling audit trails aids in establishing the accountability and responsibility for processed transactions by tracing them through the information system. Enabling audit trails increases the use of disk space. A transaction log file would be used totrace transactions, but would not aid in determining accountability and responsibility. The objective of capacity planning is the efficient and effective use of IT resources and requires information such as CPU utilization, bandwidth, number of users, etc.

NEW QUESTION 362
- (Topic 4)
Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

A. System testing
B. Acceptance testing

C. Integration testing
D. Unit testing

Answer: B

Explanation:

Acceptance testing is the final stage before the software is installed and is available for use. The greatest impact would occur if the software fails at the acceptance testing level, as this could result in delays and cost overruns. System testing is undertaken by the developer team to determine if the software meets user requirements per specifications. Integration testing examines the units/modules as one integrated system and unit testing examines the individual units or components of the software. System, integration and unit testing are all performed by the developers at various stages of development; the impact of failure is comparatively less for each than failure at the acceptance testing stage.

NEW QUESTION 363
- (Topic 4)
Which of the following is an object-oriented technology characteristic that permits an enhanced degree of security over data?

A. inheritance
B. Dynamic warehousing
C. Encapsulation
D. Polymorphism

Answer: C

Explanation:

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

NEW QUESTION 367
- (Topic 4)
Which of the following is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality?

A. Function point analysis
B. Critical path methodology
C. Rapid application development
D. Program evaluation review technique

Answer: C

Explanation:

Rapid application development is a management technique that enables organizations to develop strategically important systems faster, while reducing development costs and maintaining quality. The program evaluation review technique (PERT) and critical path methodology (CPM) are both planning and control techniques, while function point analysis is used for estimating the complexity of developing business applications.

NEW QUESTION 370
- (Topic 4)
Which of the following is the PRIMARY purpose for conducting parallel testing?

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

Answer: D

Explanation:

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

NEW QUESTION 375
- (Topic 4)
The use of object-oriented design and development techniques would MOST likely:

A. facilitate the ability to reuse module
B. improve system performanc
C. enhance control effectivenes
D. speed up the system development life cycl

Answer: A

Explanation:

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

NEW QUESTION 380
- (Topic 4)
Which of the following should be included in a feasibility study for a project to implement an EDI process?

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

Answer: C

Explanation:

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

NEW QUESTION 384
- (Topic 4)
Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

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

Answer: B

Explanation:

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

NEW QUESTION 389
- (Topic 4)
An IS auditor reviewing a proposed application software acquisition should ensure that the:

A. operating system (OS) being used is compatible with the existing hardware platfor
B. planned OS updates have been scheduled to minimize negative impacts on company need
C. OS has the latest versions and update
D. products are compatible with the current or planned O

Answer: D

Explanation:

Choices A, B and C are incorrect because none of them are related to the area being audited. In reviewing the proposed application the auditor should ensure that the products to be purchased are compatible with the current or planned OS. Regarding choice A, if the OS is currently being used, it is compatible with the existing hardware platform, because if it is not it would not operate properly. In choice B, the planned OS updates should be scheduled to minimize negative impacts on the organization. For choice C, the installed OS should be equipped with the most recent versions and updates (with sufficient history and stability).

NEW QUESTION 393
- (Topic 4)
Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

A. Bottom up
B. Sociability testing
C. Top-down
D. System test

Answer: C

Explanation:

The top-down approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early. A bottom-up approach to testing begins with atomic units, such as programs and modules, and works upward until acomplete system test has taken place. Sociability testing and system tests take place at a later stage in the development process.

NEW QUESTION 396
- (Topic 4)
Which of the following is an advantage of the top-down approach to software testing?

A. Interface errors are identified early
B. Testing can be started before all programs are complete

C. it is more effective than other testing approaches
D. Errors in critical modules are detected sooner

Answer: A

Explanation:

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

NEW QUESTION 401
- (Topic 4)
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

A. increase the time allocated for system testing
B. implement formal software inspections
C. increase the development staff
D. Require the sign-off of all project deliverables

Answer: B

Explanation:

Inspections of code and design are a proven software quality technique. An advantage of this approach is that defects are identified before they propagate through the development life cycle. This reduces the cost of correction as less rework is involved. Allowing more time for testing may discover more defects; however, little is revealed as to why the quality problems are occurring and the cost of the extra testing, and the cost of rectifying the defects found will be greater than if they had been discovered earlier in the development process. The ability of the development staff can have a bearing on the quality of what is produced; however, replacing staff can be expensive and disruptive, and the presence of a competent staff cannot guarantee quality in the absence of effective quality management processes. Sign-off of deliverables may help detect defects if signatories are diligent about reviewing deliverable content; however, this is difficult to enforce. Deliverable reviews normally do not go down to the same level of detail as software inspections.

NEW QUESTION 406
- (Topic 4)
Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

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

Answer: A

Explanation:

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

NEW QUESTION 407
- (Topic 4)
The reason a certification and accreditation process is performed on critical systems is to ensure that:

A. security compliance has been technically evaluate
B. data have been encrypted and are ready to be store
C. the systems have been tested to run on different platform
D. the systems have followed the phases of a waterfall mode

Answer: A

Explanation:

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

NEW QUESTION 409
- (Topic 4)
An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transaction
B. implement before-and-after image reportin
C. Use tracing and taggin
D. implement integrity constraints in the databas

Answer: D

Explanation:

Implementing integrity constraints in the database is a preventive control, because data is checked against predefined tables or rules preventing any undefined data from being entered. Logging all table update transactions and implementing before-and-after image reporting are detective controls that would not avoid the situation. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.

NEW QUESTION 413
- (Topic 4)
Responsibility and reporting lines cannot always be established when auditing automated systems since:

A. diversified control makes ownership irrelevan
B. staff traditionally changes jobs with greater frequenc
C. ownership is difficult to establish where resources are share
D. duties change frequently in the rapid development of technolog

Answer: C

Explanation:

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

NEW QUESTION 418
- (Topic 4)
Which of the following represents the GREATEST potential risk in an EDI environment?

A. Transaction authorization
B. Loss or duplication of EDI transmissions
C. Transmission delay
D. Deletion or manipulation of transactions prior to or after establishment of application controls

Answer: A

Explanation:

Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk. Choices B and D are examples of risks, but the impact is not as great as that of unauthorized transactions. Transmission delays may terminate the process or hold the line until the normal time for processing has elapsed; however, there will be no loss of data.

NEW QUESTION 423
- (Topic 4)
The GREATEST advantage of using web services for the exchange of information between two systems is:

A. secure communication
B. improved performanc
C. efficient interfacin
D. enhanced documentatio

Answer: C

Explanation:

Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

NEW QUESTION 427
- (Topic 4)
When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

A. excessive transaction turnaround tim
B. application interface failur
C. improper transaction authorizatio
D. nonvalidated batch total

Answer: C

Explanation:

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

NEW QUESTION 428
- (Topic 5)
Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

Answer: D

Explanation:

IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes. Utilization reports document the use of computer equipment, and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

NEW QUESTION 431
- (Topic 5)
Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?

A. Minimizing costs for the services provided
B. Prohibiting the provider from subcontracting services
C. Evaluating the process for transferring knowledge to the IT department
D. Determining if the services were provided as contracted

Answer: D

Explanation:

From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need) is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department. Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

NEW QUESTION 433
- (Topic 5)
Which of the following will help detect changes made by an intruder to the system log of a server?

A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite

Answer: B

Explanation:

A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

NEW QUESTION 435
- (Topic 5)
Which of the following BEST ensures the integrity of a server's operating system?

A. Protecting the server in a secure location
B. Setting a boot password
C. Hardening the server configuration
D. Implementing activity logging

Answer: C

Explanation:

Hardening a system means to configure it in the most secure manner (install latest security patches, properly define the access authorization for users and administrators, disable insecure options and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario-it is a detective control (not a preventive one), and the attacker who already gained privileged accesscan modify logs or disable them.

NEW QUESTION 440
- (Topic 5)
The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:

A. compression software to minimize transmission duratio
B. functional or message acknowledgment
C. a packet-filtering firewall to reroute message
D. leased asynchronous transfer mode line

Answer: D

Explanation:

Leased asynchronous transfer mode lines are a way to avoid using public and shared infrastructures from the carrier or Internet service provider that have a greater number of communication failures. Choice A, compression software, is a valid way to reduce the problem, but is not as good as leased asynchronous transfer mode lines. Choice B is a control based on higher protocol layers and helps if communication lines are introducing noise, but not if a link is down. Choice C, a packet-filtering firewall, does not reroute messages.

NEW QUESTION 444
- (Topic 5)
An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:

A. source documentation retentio
B. data file securit
C. version usage contro
D. one-for-one checkin

Answer: C

Explanation:

For processing to be correct, it is essential that the proper version of a file is used. Transactions should be applied to the most current database, while restart procedures should use earlier versions. Source documentation should be retained for anadequate time period to enable documentation retrieval, reconstruction or verification of data, but it does not aid in ensuring that the correct version of a file will be used. Data file security controls prevent access by unauthorized users who could then alter the data files; however, it does not ensure that the correct file will be used. It is necessary to ensure that all documents have been received for processing, one-for-one; however, this does not ensure the use of the correct file.

NEW QUESTION 445
- (Topic 5)
Which of the following BEST limits the impact of server failures in a distributed environment?

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

Answer: B

Explanation:

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

NEW QUESTION 446
- (Topic 5)
An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?

A. Staging and job set up
B. Supervisory review of logs
C. Regular back-up of tapes
D. Offsite storage of tapes

Answer: A

Explanation:

If the IS auditor finds that there are effective staging and job set up processes, this can be accepted as a compensating control. Choice B is a detective control while choices C and D are corrective controls, none of which would serve as good compensating controls.

NEW QUESTION 449
- (Topic 5)
The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized user
B. prevent integrity problems when two processes attempt to update the same data at the same tim
C. prevent inadvertent or unauthorized disclosure of data in the databas
D. ensure the accuracy, completeness and consistency of dat

Answer: B

Explanation:

Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time. Access controls restrict updating of the database to authorized users, and controls such as passwords preventthe inadvertent or unauthorized disclosure of data from the database. Quality controls, such as edits, ensure the accuracy, completeness and consistency of data maintained in the database.

NEW QUESTION 454
- (Topic 5)

An IS auditor finds that client requests were processed multiple times when received
from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

A. increase the frequency for data replication between the different department systems to ensure timely update
B. Centralize all request processing in one department to avoid parallel processing of the same reques
C. Change the application architecture so that common data are held in just one shared database for all department
D. implement reconciliation controls to detect duplicates before orders are processed in the system

Answer: C

Explanation:

Keeping the data in one place is the best way to ensure that data are stored without redundancy and that all users have the same data on their systems. Although increasing the frequency may help to minimize the problem, the risk of duplication cannotbe eliminated completely because parallel data entry is still possible. Business requirements will most likely dictate where data processing activities are performed. Changing the business structure to solve an IT problem is not practical or politically feasible. Detective controls do not solve the problem of duplicate processing, and would require that an
additional process be implemented to handle the discovered duplicates.

NEW QUESTION 455
- (Topic 5)
An IS auditor finds that, at certain times of the day, the data warehouse query
performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

A. Permanent table-space allocation
B. Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls

Answer: C

Explanation:

User spool limits restrict the space available for running user queries. This prevents poorly formed queries from consuming excessive system resources and impacting general query performance. Limiting the space available to users in their own databases prevents them from building excessively large tables. This helps to control space utilization which itself acts to help performance by maintaining a buffer between the actual data volume stored and the physical device capacity. Additionally, it prevents users from consuming excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run overnight and are optimized for performance purposes), in a data warehouse, since you are not running online transactions, commitment and rollback does not have an impact on performance. The other choices are not as likely to be the root cause of this performance issue.

NEW QUESTION 459
- (Topic 5)
Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

A. Parity check
B. Echo check
C. Block sum check
D. Cyclic redundancy check

Answer: D

Explanation:

The cyclic redundancy check (CRC) can check for a block of transmitted datA. The workstations generate the CRC and transmit it with the datA. The receiving workstation computes a CRC and compares it to the transmitted CRC. if both of them are equal.then the block is assumed error free, in this case (such as in parity error or echo check), multiple errors can be detected. In general, CRC can detect all single-bit and bubble-bit errors. Parity check (known as vertical redundancy check) also involves adding a bit (known as the parity bit) to each character during transmission. In this case, where there is a presence of bursts of errors (i.e., impulsing noise during high transmission rates), it has a reliability of approximately 50 percent. Inhigher transmission rates, this limitation is significant. Echo checks detect line errors by retransmitting data to the sending device for comparison with the original transmission.

NEW QUESTION 460
- (Topic 5)
Which of the following types of firewalls provide the GREATEST degree and granularity of control?

A. Screening router
B. Packet filter
C. Application gateway
D. Circuit gateway

Answer: C

Explanation:

The application gateway is similar to a circuit gateway, but it has specific proxies for each service. To handle web services, it has an HTTP proxy that acts as an intermediary between externals and internals, but is specifically for HTTP. This meansthat it not only checks the packet IP addresses (layer 3) and the ports it is directed to (in this case port 80, or layer 4), it also checks every HTTP command (layers 5 and 7). Therefore, it works in a more detailed (granularity) way than the others. Screening router and packet filter (choices A and BJ work at the protocol, service and/or port level. This means that they analyze packets from layers 3 and 4, and not from higher levels. A circuit gateway (choice D) is based on a proxy or programthat acts as an intermediary between external and internal accesses. This means that during an external access, instead of opening a single connection to the internal server, two connections are established-one from the external server to the proxy(which conforms the circuit-gateway) and one from the proxy to the internal server. Layers 3 and 4 (IP and TCP) and some general features from higher protocols are used to perform these tasks.

NEW QUESTION 461

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CISA Exam with Our Prep Materials Via below:

https://www.certleader.com/CISA-dumps.html