Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (Topic 1)
Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

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

Answer: D

Explanation:

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

NEW QUESTION 2
- (Topic 1)
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)
Structured programming is BEST described as a technique that:

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

Answer: B

Explanation:

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

NEW QUESTION 4
- (Topic 1)
Which of the following network configuration options contains a direct link between any two host machines?

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

Answer: D

Explanation:

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

NEW QUESTION 5
- (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 6
- (Topic 1)
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

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

Answer: B

Explanation:

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

NEW QUESTION 7
- (Topic 1)
A critical function of a firewall is to act as a:

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

Answer: B

Explanation:

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

NEW QUESTION 8
- (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 9
- (Topic 1)
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

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

Answer: A

Explanation:

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

NEW QUESTION 10
- (Topic 1)

A hub is a device that connects:

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

Answer: D

Explanation:

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

NEW QUESTION 10
- (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 11
- (Topic 1)
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

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

Answer: C

Explanation:

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

NEW QUESTION 15
- (Topic 1)
The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

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

Answer: B

Explanation:

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

NEW QUESTION 18
- (Topic 1)
After an IS auditor has identified threats and potential impacts, the auditor should:

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

Answer: A

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

NEW QUESTION 19
- (Topic 1)
What type of risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist?

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

Answer: B

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

NEW QUESTION 24
- (Topic 1)
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

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

Answer: D

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

NEW QUESTION 28
- (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 30
- (Topic 1)
Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 34
- (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 36
- (Topic 1)
An IS auditor usually places more reliance on evidence directly collected. What is an example of such evidence?

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

Answer: A

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

NEW QUESTION 40
- (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 41
- (Topic 1)
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 46
- (Topic 1)
Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

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

Answer: C

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

NEW QUESTION 49
- (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 52
- (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 53
- (Topic 1)
Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

A. Assigning user access privileges
B. Developing organizational security policies
C. Creating roles and responsibilities
D. Classifying data

Answer: D

Explanation:
To properly implement data classification, establishing data ownership is an important first step.

NEW QUESTION 55
- (Topic 1)
What influences decisions regarding criticality of assets?

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

Answer: C

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

NEW QUESTION 56
- (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 57
- (Topic 1)
Run-to-run totals can verify data through which stage(s) of application processing?

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

Answer: B

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

NEW QUESTION 61
- (Topic 1)
Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 66

- (Topic 1)
A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

A. Deletion
B. Input
C. Access
D. Duplication

Answer: B

Explanation:
A transaction journal provides the information necessary for detecting unauthorized input from a terminal.

NEW QUESTION 68
- (Topic 1)
An intentional or unintentional disclosure of a password is likely to be evident within control logs. True or false?

A. True
B. False

Answer: B

Explanation:
An intentional or unintentional disclosure of a password is not likely to be evident within control logs.

NEW QUESTION 70
- (Topic 1)
When are benchmarking partners identified within the benchmarking process?

A. In the design stage
B. In the testing stage
C. In the research stage
D. In the development stage

Answer: C

Explanation:
Benchmarking partners are identified in the research stage of the benchmarking process.

NEW QUESTION 73
- (Topic 1)
A check digit is an effective edit check to:

A. Detect data-transcription errors
B. Detect data-transposition and transcription errors
C. Detect data-transposition, transcription, and substitution errors
D. Detect data-transposition errors

Answer: B

Explanation:
A check digit is an effective edit check to detect data-transposition and transcription errors.

NEW QUESTION 75
- (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 78
- (Topic 1)
Which of the following is of greatest concern to the IS auditor?

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

Answer: A

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

NEW QUESTION 82
- (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 87
- (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 88
- (Topic 1)
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 93
- (Topic 1)
What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 97
- (Topic 1)
Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

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

Answer: C

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

NEW QUESTION 101

- (Topic 1)
Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem? Choose the BEST answer.

A. Expert systems
B. Neural networks
C. Integrated synchronized systems
D. Multitasking applications

Answer: B

Explanation:
Neural networks are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem.

NEW QUESTION 104
- (Topic 1)
What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

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

Answer: C

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

NEW QUESTION 106
- (Topic 1)
What is/are used to measure and ensure proper network capacity management and availability of services? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 110
- (Topic 1)
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

A. Traffic analysis
B. SYN flood
C. Denial of service (DoS)
D. Distributed denial of service (DoS)

Answer: A

Explanation:
Traffic analysis is a passive attack method used by intruders to determine potential network vulnerabilities. All others are active attacks.

NEW QUESTION 113
- (Topic 1)
What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

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

Answer: A

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

NEW QUESTION 118
- (Topic 1)
What should IS auditors always check when auditing password files?

A. That deleting password files is protected
B. That password files are encrypted
C. That password files are not accessible over the network
D. That password files are archived

Answer: B

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

NEW QUESTION 120
- (Topic 1)
Which of the following is the most fundamental step in preventing virus attacks?

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

Answer: A

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

NEW QUESTION 125
- (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 129
- (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 131
- (Topic 1)
What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

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

Answer: C

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

NEW QUESTION 135
- (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 136
- (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 141
- (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 143
- (Topic 1)
Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

A. Failing to perform user acceptance testing
B. Lack of user training for the new system
C. Lack of software documentation and run manuals
D. Insufficient unit, module, and systems testing

Answer: A

Explanation:
Above almost all other concerns, failing to perform user acceptance testing often results in the greatest negative impact on the implementation of new application software.

NEW QUESTION 147
- (Topic 1)
After identifying potential security vulnerabilities, what should be the IS auditor's next step?

A. To evaluate potential countermeasures and compensatory controls
B. To implement effective countermeasures and compensatory controls
C. To perform a business impact analysis of the threats that would exploit the vulnerabilities
D. To immediately advise senior management of the findings

Answer: C

Explanation:
After identifying potential security vulnerabilities, the IS auditor's next step is to perform a business impact analysis of the threats that would exploit the vulnerabilities.

NEW QUESTION 149
- (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 150
- (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 153
- (Topic 2)
Which of the following sampling methods is MOST useful when testing for compliance?

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

Answer: A

Explanation:

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

NEW QUESTION 158
- (Topic 2)
Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

A. Multiple cycles of backup files remain availabl
B. Access controls establish accountability for e-mail activit
C. Data classification regulates what information should be communicated via e-mai
D. Within the enterprise, a clear policy for using e-mail ensures that evidence is availabl

Answer: A

Explanation:

Backup files containing documents that supposedly have been deleted could be recovered from these files. Access controls may help establish accountability for the issuance of a particular document, but this does not provide evidence of the e-mail. Data classification standards may be in place with regards to what should be communicated via e-mail, but the creation of the policy does not provide the information required for litigation purposes.

NEW QUESTION 159
- (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 162
- (Topic 2)
An organization's IS audit charter should specify the:

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

Answer: D

Explanation:

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

NEW QUESTION 164
- (Topic 2)
An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

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

Answer: D

Explanation:

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

NEW QUESTION 166
- (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 167
- (Topic 2)
When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

A. sufficient evidence will be collecte
B. all significant deficiencies identified will be corrected within a reasonable perio
C. all material weaknesses will be identifie
D. audit costs will be kept at a minimum leve

Answer: A

Explanation:

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

NEW QUESTION 170
- (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 173
- (Topic 2)
The PRIMARY purpose of an IT forensic audit is:

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

Answer: B

Explanation:

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

NEW QUESTION 175
- (Topic 2)
An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

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

Answer: D

Explanation:

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

NEW QUESTION 179
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 180
- (Topic 2)
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

Answer: A

Explanation:

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

NEW QUESTION 182
- (Topic 2)
An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

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

Answer: A

Explanation:

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

NEW QUESTION 184
- (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 188
- (Topic 2)
Which of the following is an advantage of an integrated test facility (ITF)?

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

Answer: B

Explanation:

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

NEW QUESTION 191
- (Topic 2)
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

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

Answer: C

Explanation:

An IS auditor should next examine cases where incorrect calculations occurred and confirm the results. After the calculations have been confirmed, further tests can be conducted and reviewed. Report preparation, findings and recommendations would notbe made until all results are confirmed.

NEW QUESTION 195
- (Topic 2)
An IS auditor performing a review of an application's controls would evaluate the:

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

Answer: B

Explanation:

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

NEW QUESTION 196
- (Topic 2)
While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

A. Observe the response mechanis

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

Answer: C

Explanation:

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

NEW QUESTION 198
- (Topic 2)
A substantive test to verify that tape library inventory records are accurate is:

A. determining whether bar code readers are installe
B. determining whether the movement of tapes is authorize
C. conducting a physical count of the tape inventor
D. checking if receipts and issues of tapes are accurately recorde

Answer: C

Explanation:

A substantive test includes gathering evidence to evaluate the integrity of individual transactions, data or other information. Conducting a physical count of the tape inventory is a substantive test. Choices A, B and D are compliance tests.

NEW QUESTION 201
- (Topic 2)
An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

A. professional independence
B. organizational independenc
C. technical competenc
D. professional competenc

Answer: A

Explanation:

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

NEW QUESTION 204
- (Topic 2)
The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

A. understand the business proces
B. comply with auditing standard
C. identify control weaknes
D. plan substantive testin

Answer: A

Explanation:

Understanding the business process is the first step an IS auditor needs to perform. Standards do not require an IS auditor to perform a process walkthrough. Identifying control weaknesses is not the primary reason for the walkthrough and typically occurs at a later stage in the audit, while planning for substantive testing is performed at a later stage in the audit.

NEW QUESTION 206
- (Topic 2)
The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

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

Answer: B

Explanation:

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

NEW QUESTION 211
- (Topic 2)
Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

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

Answer: C

Explanation:

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

NEW QUESTION 214
- (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 216
- (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)
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 222
- (Topic 2)
The success of control self-assessment (CSA) highly depends on:

A. having line managers assume a portion of the responsibility for control monitorin
B. assigning staff managers the responsibility for building, but not monitoring, control
C. the implementation of a stringent control policy and rule-driven control

D. the implementation of supervision and the monitoring of controls of assigned dutie

Answer: A

Explanation:

The primary objective of a CSA program is to leverage the internal audit function by shifting some of the control monitoring responsibilities to the functional area line managers. The success of a control self-assessment (CSA) program depends on thedegree to which line managers assume responsibility for controls- Choices B, C and D are characteristics of a traditional audit approach, not a CSA approach.

NEW QUESTION 223
- (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 229
- (Topic 3)
An IS steering committee should:

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

Answer: C

Explanation:

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

NEW QUESTION 232
- (Topic 3)
IT governance is PRIMARILY the responsibility of the:

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

Answer: B

Explanation:

IT governance is primarily the responsibility of the executives and shareholders {as represented by the board of directors). The chief executive officer is

instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

NEW QUESTION 234
- (Topic 3)
As an outcome of information security governance, strategic alignment provides:

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

Answer: A

Explanation:

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

NEW QUESTION 239
- (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 244
- (Topic 3)
When implementing an IT governance framework in an organization the MOST important objective is:

A. IT alignment with the busines
B. accountabilit
C. value realization with I
D. enhancing the return on IT investment

Answer: A

Explanation:

The goals of IT governance are to improve IT performance, to deliver optimum business value and to ensure regulatory compliance. The key practice in support of these goals is the strategic alignment of IT with the business {choice A). To achieve alignment, all other choices need to be tied to business practices and strategies.

NEW QUESTION 247
- (Topic 3)
When an employee is terminated from service, the MOST important action is to:

A. hand over all of the employee's files to another designated employe
B. complete a backup of the employee's wor
C. notify other employees of the terminatio
D. disable the employee's logical acces

Answer: D

Explanation:

There is a probability that a terminated employee may misuse access rights; therefore, disabling the terminated employee's logical access is the most important action to take. All the work of the terminated employee needs to be handed over to a designated employee; however, this should be performed after implementing choice D. All the work of the terminated employee needs to be backed up and the employees need to be notified of the termination of the employee, but this should not precede the action in choice D.

NEW QUESTION 250
- (Topic 3)
Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivit

B. reduce the opportunity for an employee to commit an improper or illegal ac
C. provide proper cross-training for another employe
D. eliminate the potential disruption caused when an employee takes vacation one day at a tim

Answer: B

Explanation:

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

NEW QUESTION 253
- (Topic 3)
When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

A. Restricting physical access to computing equipment
B. Reviewing transaction and application logs
C. Performing background checks prior to hiring IT staff
D. Locking user sessions after a specified period of inactivity

Answer: B

Explanation:

Only reviewing transaction and application logs directly addresses the threat posed by poor segregation of duties. The review is a means of detecting inappropriate behavior and also discourages abuse, because people who may otherwise be tempted to exploit the situation are aware of the likelihood of being caught. Inadequate segregation of duties is more likely to be exploited via logical access to data and computing resources rather than physical access. Choice C is a useful control to ensure ITstaff are trustworthy and competent but does not directly address the lack of an optimal segregation of duties. Choice D acts to prevent unauthorized users from gaining system access, but the issue of a lack of segregation of duties is more the misuse (deliberately or inadvertently} of access privileges that have officially been granted.

NEW QUESTION 254
- (Topic 3)
To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

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

Answer: B

Explanation:

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

NEW QUESTION 257
- (Topic 3)
In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

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

Answer: A

Explanation:

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

NEW QUESTION 258
- (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 260
- (Topic 3)
When reviewing an organization's strategic IT plan an IS auditor should expect to find:

A. an assessment of the fit of the organization's application portfolio with business objective
B. actions to reduce hardware procurement cos
C. a listing of approved suppliers of IT contract resource
D. a description of the technical architecture for the organization's network perimeter securit

Answer: A

Explanation:

An assessment of how well an organization's application portfolio supports the organization's business objectives is a key component of the overall IT strategic planning process. This drives the demand side of IT planning and should convert into a set of strategic IT intentions. Further assessment can then be made of how well the overall IT organization, encompassing applications, infrastructure, services, management processes, etc., can support the business objectives. Operational efficiency initiatives belong to tactical planning, not strategic planning. The purpose of an IT strategic plan is toset out how IT will be used to achieve or support an organization's business objectives. A listing of approved suppliers of IT contract resources is a tactical rather than a strategic concern. An IT strategic plan would not normally include detail ofa specific technical architecture.

NEW QUESTION 264
- (Topic 3)
The rate of change in technology increases the importance of:

A. outsourcing the IS functio
B. implementing and enforcing good processe
C. hiring personnel willing to make a career within the organizatio
D. meeting user requirement

Answer: B

Explanation:

Change requires that good change management processes be implemented and enforced. Outsourcing the IS function is not directly related to the rate of technological change. Personnel in a typical IS department are highly qualified and educated; usually they do not feel their jobs are at risk and are prepared to switch jobs frequently. Although meeting user requirements is important, it is not directly related to the rate of technological change in the IS environment.

NEW QUESTION 266
- (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 267
- (Topic 3)
A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

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

Answer: B

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the officialform of classic 'paper* makes the retention of corporate e-mail a

necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

NEW QUESTION 272
- (Topic 3)
An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

A. report that the control is operating effectively since deactivation happens within the time frame stated in the IS polic
B. verify that user access rights have been granted on a need-to-have basi
C. recommend changes to the IS policy to ensure deactivation of user IDs upon terminatio
D. recommend that activity logs of terminated users be reviewed on a regular basi

Answer: C

Explanation:

Although a policy provides a reference for performing IS audit assignments, an IS auditor needs to review the adequacy and the appropriateness of the policy. If, in the opinion of the auditor, the time frame defined for deactivation is inappropriate,the auditor needs to communicate this to management and recommend changes to the policy. Though the deactivation happens as stated in the policy, it cannot be concluded that the control is effective. Best practice would require that the ID of a terminated user be deactivated immediately. Verifying that user access rights have been granted on a need-to-have basis is necessary when permissions are granted. Recommending that activity logs of terminated users be reviewed on a regular basis is a good practice, but not as effective as deactivation upon termination.

NEW QUESTION 276
- (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 281
- (Topic 3)
In the context of effective information security governance, the primary objective of value delivery is to:

A. optimize security investments in support of business objective
B. implement a standard set of security practice
C. institute a standards-based solutio
D. implement a continuous improvement cultur

Answer: A

Explanation:

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

NEW QUESTION 284
- (Topic 3)
After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

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

Answer: B

Explanation:

The efforts should be consolidated to ensure alignment with the overall strategy of the postmerger organization. If resource allocation is not centralized, the separate projects are at risk of overestimating the availability of key knowledge resources for the in-house developed legacy applications. In postmerger integration programs, it is common to form project management offices to ensure standardized and comparable information levels in the planning and reporting structures, and to centralizedependencies of project deliverables or resources. The experience of external consultants can be valuable since project management practices do not require in-depth knowledge of the legacy systems. This can free up resources for functional tasks. Itis a good idea to first get familiar with the old systems,

to understand what needs to be done in a migration and to evaluate the implications of technical decisions. In most cases, mergers result in application changes and thus in training needs asorganizations and processes change to leverage the intended synergy effects of the merger.

NEW QUESTION 285
- (Topic 3)
An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

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

Answer: C

Explanation:

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

NEW QUESTION 287
- (Topic 3)
To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

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

Answer: B

Explanation:

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

NEW QUESTION 292
- (Topic 3)
When an organization is outsourcing their information security function, which of the following should be kept in the organization?

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

Answer: A

Explanation:

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

NEW QUESTION 293
- (Topic 3)
An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

A. That an audit clause is present in all contracts
B. That the SLA of each contract is substantiated by appropriate KPIs
C. That the contractual warranties of the providers support the business needs of the organization
D. That at contract termination, support is guaranteed by each outsourcer for new outsourcers

Answer: C

Explanation:

The complexity of IT structures matched by the complexity and interplay of responsibilities and warranties may affect or void the effectiveness of those warranties and the reasonable certainty that the business needs will be met. All other choices are important, but not as potentially dangerous as the interplay of the diverse and critical areas of the contractual responsibilities of the outsourcers.

NEW QUESTION 294
- (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 296
- (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 300
- (Topic 3)
The output of the risk management process is an input for making:

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

Answer: C

Explanation:

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

NEW QUESTION 304
- (Topic 3)
When developing a risk management program, what is the FIRST activity to be performed?

A. Threat assessment
B. Classification of data
C. Inventory of assets
D. Criticality analysis

Answer: C

Explanation:

Identification of the assets to be protected is the first step in the development of a risk management program. A listing of the threats that can affect the performance of these assets and criticality analysis are later steps in the process. Data classification is required for defining access controls and in criticality analysis.

NEW QUESTION 305
- (Topic 3)
Which of the following does a lack of adequate security controls represent?

A. Threat
B. Asset
C. Impact
D. Vulnerability

Answer: D

Explanation:

The lack of adequate security controls represents a vulnerability, exposing sensitive information and data to the risk of malicious damage, attack or unauthorized access by hackers. This could result in a loss of sensitive information and lead to theloss of goodwill for the organization. A succinct definition of risk is provided by the Guidelines for the Management of IT Security published by the International Organization for Standardization (ISO), which defines risk as the 'potential that a given threat will exploit the vulnerability of an asset or group of assets to cause loss or damage to the assets.' The various elements of the definition are vulnerability, threat, asset and impact. Lack of adequate security functionalityin this context is a vulnerability.

NEW QUESTION 306
- (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 311
- (Topic 3)
Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

A. Process maturity
B. Performance indicators
C. Business risk
D. Assurance reports

Answer: C

Explanation:

Priority should be given to those areas which represent a known risk to the enterprise's operations. The level of process maturity, process performance and audit reports will feed into the decision making process. Those areas that represent real risk to the business should be given priority.

NEW QUESTION 315
- (Topic 3)
During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

A. Create an IT risk management department and establish an IT risk framework with the aid of external risk management expert
B. Use common industry standard aids to divide the existing risk documentation into several individual risks which will be easier to handl
C. No recommendation is necessary since the current approach is appropriate for a medium-sized organizatio
D. Establish regular IT risk management meetings to identify and assess risks, and create a mitigation plan as input to the organization's risk managemen

Answer: D

Explanation:

Establishing regular meetings is the best way to identify and assess risks in a medium-sized organization, to address responsibilities to the respective management and to keep the risk list and mitigation plans up to date. A medium-sized organizationwould normally not have a separate IT risk management department. Moreover, the risks are usually manageable enough so that external help would not be needed. While common risks may be covered by common industry standards, they cannot address the specific situation of an organization. Individual risks will not be discovered without a detailed assessment from within the organization. Splitting the one risk position into several is not sufficient.

NEW QUESTION 319
- (Topic 4)
Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

A. Project database
B. Policy documents
C. Project portfolio database
D. Program organization

Answer: C

Explanation:

A project portfolio database is the basis for project portfolio management. It includes project data, such as owner, schedules, objectives, project type, status and cost. Project portfolio management requires specific project portfolio reports. A project database may contain the above for one specific project and updates to various parameters pertaining to the current status of that single project. Policy documents on project management set direction for the design, development,

implementation and monitoring of the project. Program organization is the team required (steering committee, quality assurance, systems personnel, analyst, programmer, hardware support, etc.) to meet the delivery objective of the project.

NEW QUESTION 323
- (Topic 4)
When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

A. whose sum of activity time is the shortes
B. that have zero slack tim
C. that give the longest possible completion tim
D. whose sum of slack time is the shortes

Answer: B

Explanation:

A critical path's activity time is longer than that for any other path through the network. This path is important because if everything goes as scheduled, its length gives the shortest possible completion time for the overall project. Activities onthe critical path become candidates for crashing, i.e., for reduction in their time by payment of a premium for early completion. Activities on the critical path have zero slack time and conversely, activities with zero slack time are on a critical path. By successively relaxing activities on a critical path, a curve showing total project costs vs. time can be obtained.

NEW QUESTION 326
- (Topic 4)
An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impactingthe project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

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

Answer: A

Explanation:

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

NEW QUESTION 331
- (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 335
- (Topic 4)
An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

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

Answer: C

Explanation:

A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results. A project sponsor is typically the senior manager in charge of the primary business unit that the

application will support. The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics forthe project. The project sponsor is not responsible for reviewing the progress of the project. A system development project team (SDPT) completes the assigned tasks, works according to the instructions of the project manager and communicates with the user project team. The SDPT is not responsible for reviewing the progress of the project. A user project team (UPT) completes the assigned tasks, communicates effectively with the system development team and works according to the advice of the project manager. A UPT is not responsible for reviewing the progress of the project.

NEW QUESTION 340
- (Topic 4)
A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

A. what amount of progress against schedule has been achieve
B. if the project budget can be reduce
C. if the project could be brought in ahead of schedul
D. if the budget savings can be applied to increase the project scop

Answer: A

Explanation:

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

NEW QUESTION 341
- (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 346
- (Topic 4)
What control detects transmission errors by appending calculated bits onto the end of each segment of data?

A. Reasonableness check
B. Parity check
C. Redundancy check
D. Check digits

Answer: C

Explanation:

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

NEW QUESTION 347
- (Topic 4)
Which of the following will BEST ensure the successful offshore development of business applications?

A. Stringent contract management practices
B. Detailed and correctly applied specifications
C. Awareness of cultural and political differences
D. Postimplementation reviews

Answer: B

Explanation:

When dealing with offshore operations, it is essential that detailed specifications be created. Language differences and a lack of interaction between developers and physically remote end users could create gaps in communication in which assumptionsand modifications may not be adequately communicated. Contract management practices, cultural and political differences, and postimplementation reviews, although important, are not as pivotal to the success of the project.

NEW QUESTION 352
- (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 357
- (Topic 4)
An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

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

Answer: C

Explanation:

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

NEW QUESTION 360
- (Topic 4)
An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

A. continuous improvemen
B. quantitative quality goal
C. a documented proces
D. a process tailored to specific project

Answer: A

Explanation:

An organization would have reached the highest level of the software CMM at level 5, optimizing. Quantitative quality goals can be reached at level 4 and below, a documented process is executed at level 3 and below, and a process tailored to specific projects can be achieved at level 3 or below.

NEW QUESTION 361
- (Topic 4)
Which of the following is a dynamic analysis tool for the purpose of testing software modules?

A. Black box test
B. Desk checking
C. Structured walkthrough
D. Design and code

Answer: A

Explanation:

A black box test is a dynamic analysis tool for testing software modules. During the testing of software modules a black box test works first in a cohesive manner as a single unit/entity consisting of numerous modules, and second with the user data that flows across software modules, in some cases, this even drives the software behavior. In choices B, C and D, the software (design or code) remains static and someone closely examines it by applying their mind, without actually activating the software. Therefore, these cannot be referred to as dynamic analysis tools.

NEW QUESTION 363
- (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 365
CORRECT TEXT - (Topic 4)
Which of the following is an advantage of prototyping?

A. The finished system normally has strong internal control
B. Prototype systems can provide significant time and cost saving
C. Change control is often less complicated with prototype system
D. it ensures that functions or extras are not added to the intended syste

Answer: B

NEW QUESTION 368
- (Topic 4)
During which of the following phases in system development would user acceptance test plans normally be prepared?

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

Answer: B

Explanation:

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

NEW QUESTION 371
- (Topic 4)
An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

A. a backup server be available to run ETCS operations with up-to-date dat
B. a backup server be loaded with all the relevant software and dat
C. the systems staff of the organization be trained to handle any even
D. source code of the ETCS application be placed in escro

Answer: D

Explanation:

Whenever proprietary application software is purchased, the contract should provide for a source code agreement. This will ensure that the purchasing company will have the opportunity to modify the software should the vendor cease to be in business.Having a backup server with current data and staff training is critical but not as critical as ensuring the availability of the source code.

NEW QUESTION 372
- (Topic 4)
During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

A. increased maintenanc
B. improper documentation of testin
C. inadequate functional testin
D. delays in problem resolutio

Answer: C

Explanation:

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

NEW QUESTION 373
- (Topic 4)

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

A. facilitates user involvemen
B. allows early testing of technical feature
C. facilitates conversion to the new syste
D. shortens the development time fram

Answer: D

Explanation:

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

NEW QUESTION 375
- (Topic 4)
The waterfall life cycle model of software development is most appropriately used when:

A. requirements are well understood and are expected to remain stable, as is the business environment in which the system will operat
B. requirements are well understood and the project is subject to time pressure
C. the project intends to apply an object-oriented design and programming approac
D. the project will involve the use of new technolog

Answer: A

Explanation:

Historically, the waterfall model has been best suited to the stable conditions described in choice A. When the degree of uncertainty of the system to be delivered and the conditions in which it will be used rises, the waterfall model has not been successful, in these circumstances, the various forms of iterative development life cycle gives the advantage of breaking down the scope of the overall system to be delivered, making the requirements gathering and design activities more manageable. Theability to deliver working software earlier also acts to alleviate uncertainty and may allow an earlier realization of benefits. The choice of a design and programming approach is not itself a determining factor of the type of software development life cycle that is appropriate. The use of new technology in a project introduces a significant element of risk. An iterative form of development, particularly one of the agile methods that focuses on early development of actual working software, is likely to be the better option to manage this uncertainty.

NEW QUESTION 378
- (Topic 4)
During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

A. buffer overflo
B. brute force attac
C. distributed denial-of-service attac
D. war dialing attac

Answer: A

Explanation:

Poorly written code, especially in web-based applications, is often exploited by hackers using buffer overflow techniques. A brute force attack is used to crack passwords. A distributed denial-of-service attack floods its target with numerous packets, to prevent it from responding to legitimate requests. War dialing uses modem-scanning tools to hack PBXs.

NEW QUESTION 380
- (Topic 4)
The MAJOR advantage of a component-based development approach is the:

A. ability to manage an unrestricted variety of data type
B. provision for modeling complex relationship
C. capacity to meet the demands of a changing environmen
D. support of multiple development environment

Answer: D

Explanation:

Components written in one language can interact with components written in other languages or running on other machines, which can increase the speed of development. Software developers can then focus on business logic. The other choices are not themost significant advantages of a component-based development approach.

NEW QUESTION 383
- (Topic 4)
Which of the following would impair the independence of a quality assurance team?

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

Answer: C

Explanation:

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

NEW QUESTION 384
- (Topic 4)
During a postimplementation review of an enterprise resource management system, an IS auditor would MOST likely:

A. review access control configuratio
B. evaluate interface testin
C. review detailed design documentatio
D. evaluate system testin

Answer: A

Explanation:

Reviewing access control configuration would be the first task performed to determine whether security has been appropriately mapped in the system. Since a postimplementation review is done after user acceptance testing and actual implementation, onewould not engage in interface testing or detailed design documentation. Evaluating interface testing would be part of the implementation process. The issue of reviewing detailed design documentation is not generally relevant to an enterprise resource management system, since these are usually vendor packages with user manuals. System testing should be performed before final user signoff.

NEW QUESTION 386
- (Topic 4)
When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

A. Use of a cryptographic hashing algorithm
B. Enciphering the message digest
C. Deciphering the message digest
D. A sequence number and time stamp

Answer: D

Explanation:

When transmitting data, a sequence number and/or time stamp built into the message to make it unique can be checked by the recipient to ensure that the message was not intercepted and replayed. This is known as replay protection, and could be used toverify that a payment instruction was not duplicated. Use of a cryptographic hashing algorithm against the entire message helps achieve data integrity. Enciphering the message digest using the sender's private key, which signs the sender's digital signature to the document, helps in authenticating the transaction. When the message is deciphered by the receiver using the sender's public key, it ensures that the message could only have come from the sender. This process of sender authentication achieves nonrepudiation.

NEW QUESTION 390
- (Topic 4)
When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. not be concerned since there may be other compensating controls to mitigate the risk
B. ensure that overrides are automatically logged and subject to revie
C. verify whether all such overrides are referred to senior management for approva
D. recommend that overrides not be permitte

Answer: B

Explanation:

If input procedures allow overrides of data validation and editing, automatic logging should occur. A management individual who did not initiate the override should review this log. An IS auditor should not assume that compensating controls exist. Aslong as the overrides are policy-compliant, there is no need for senior management approval or a blanket prohibition.

NEW QUESTION 394
- (Topic 4)
When using an integrated test facility (ITF), an IS auditor should ensure that:

A. production data are used for testin
B. test data are isolated from production dat
C. a test data generator is use
D. master files are updated with the test dat

Answer: B

Explanation:

An integrated test facility (ITF) creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live datA. While this ensures that periodic testing does not require a separate test process, there is a need to isolate test data from production datA. An IS auditor is not required to use

production data or a test data generator. Production master files should not be updated with test data.

NEW QUESTION 399
- (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 400
- (Topic 4)
When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

A. The risks associated with the use of the products are periodically assessed
B. The latest version of software is listed for each product
C. Due to licensing issues the list does not contain open source software
D. After hours support is offered

Answer: A

Explanation:

Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C andD are possible considerations but would not be the most important.

NEW QUESTION 405
- (Topic 4)
An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. authorization of program change
B. creation date of a current object modul
C. number of program changes actually mad
D. creation date of a current source progra

Answer: A

Explanation:

The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

NEW QUESTION 409
- (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 410
- (Topic 5)
Applying a retention date on a file will ensure that:

A. data cannot be read until the date is se
B. data will not be deleted before that dat

C. backup copies are not retained after that dat
D. datasets having the same name are differentiate

Answer: B

Explanation:

A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

NEW QUESTION 413
- (Topic 5)
IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

A. The outsourcing contract does not cover disaster recovery for the outsourced IT operation
B. The service provider does not have incident handling procedure
C. Recently a corrupted database could not be recovered because of library management problem
D. incident logs are not being reviewe

Answer: A

Explanation:
The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C and D are problems that should be addressed by the service provider, but are not as important as contract requirements for disaster recovery.

NEW QUESTION 418
- (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 420
- (Topic 5)
Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

A. protect the organization from viruses and nonbusiness material
B. maximize employee performanc
C. safeguard the organization's imag
D. assist the organization in preventing legal issues

Answer: A

Explanation:

The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and recreational e-mail. Choice B could be true in some circumstances (i.e., it wouldneed to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

NEW QUESTION 423
- (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 425
- (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 426
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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

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