Isaca

Exam Questions CISA

Isaca CISA

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

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

Answer: D

Explanation:

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

NEW QUESTION 2
- (Topic 1)
Which of the following is a dynamic analysis tool for the purpose of testing software modules?

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

Answer: A

Explanation:

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

NEW QUESTION 3
- (Topic 1)
Which of the following is a benefit of using callback devices?

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

Answer: A

Explanation:

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

NEW QUESTION 4
- (Topic 1)
A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

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

Answer: A

Explanation:

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

NEW QUESTION 5
- (Topic 1)
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 6
- (Topic 1)
A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

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

Answer: C

Explanation:

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

NEW QUESTION 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)
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 10
- (Topic 1)
Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

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

Answer: A

Explanation:

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

NEW QUESTION 10
- (Topic 1)
A malicious code that changes itself with each file it infects is called a:

A. logic bom
B. stealth viru
C. trojan hors
D. polymorphic viru

Answer: D

Explanation:

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

NEW QUESTION 15
- (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 19
- (Topic 1)
In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

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

Answer: A

Explanation:

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

NEW QUESTION 23
- (Topic 1)
IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 25
- (Topic 1)
A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

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

Answer: C

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

NEW QUESTION 27
- (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 31
- (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 35
- (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 36
- (Topic 1)
Which of the following best characterizes "worms"?

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

Answer: A

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

NEW QUESTION 41
- (Topic 1)
How does the SSL network protocol provide confidentiality?

A. Through symmetric encryption such as RSA
B. Through asymmetric encryption such as Data Encryption Standard, or DES
C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
D. Through symmetric encryption such as Data Encryption Standard, or DES

Answer: D

Explanation:
The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption Standard, or DES.

NEW QUESTION 44
- (Topic 1)
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 48
- (Topic 1)
When is regression testing used to determine whether new application changes have
introduced any errors in the remaining unchanged code?

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

Answer: A

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

NEW QUESTION 50
- (Topic 1)
What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 51
- (Topic 1)
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

Answer: D

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

NEW QUESTION 56
- (Topic 1)
_____ (fill in the blank) is/are are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 60
- (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 61
- (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 66
- (Topic 1)
To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 68
- (Topic 1)
Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software
B. Generalized audit software
C. Productivity audit software
D. Manual review

Answer: B

Explanation:
Generalized audit software can be used to search for address field duplications.

NEW QUESTION 73
- (Topic 1)
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 75
- (Topic 1)
Who is responsible for implementing cost-effective controls in an automated system?

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

Answer: B

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

NEW QUESTION 80
- (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 81
- (Topic 1)
When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

A. True
B. False

Answer: B

Explanation:
When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

NEW QUESTION 86
- (Topic 1)
Who should be responsible for network security operations?

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

Answer: B

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

NEW QUESTION 88
- (Topic 1)
The directory system of a database-management system describes:

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

Answer: B

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

NEW QUESTION 93

- (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 94
- (Topic 1)
What are trojan horse programs? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 95
- (Topic 1)
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

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

Answer: C

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

NEW QUESTION 97
- (Topic 1)
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

A. False
B. True

Answer: B

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

NEW QUESTION 99
- (Topic 1)
What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

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

Answer: C

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

NEW QUESTION 103
- (Topic 1)
What determines the strength of a secret key within a symmetric key cryptosystem?

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

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

Answer: B

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

NEW QUESTION 107
- (Topic 1)
What is often assured through table link verification and reference checks?

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

Answer: A

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

NEW QUESTION 111
- (Topic 1)
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 113
- (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 115
- (Topic 1)
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

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

Answer: B

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

NEW QUESTION 117
- (Topic 1)
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

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

Answer: C

Explanation:

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

NEW QUESTION 120
- (Topic 1)
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

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

Answer: A

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

NEW QUESTION 123
- (Topic 1)
When should application controls be considered within the system-development process?

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

Answer: D

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

NEW QUESTION 128
- (Topic 1)
Test and development environments should be separated. True or false?

A. True
B. False

Answer: A

Explanation:
Test and development environments should be separated, to control the stability of the test environment.

NEW QUESTION 132
- (Topic 1)
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 134
- (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 139
- (Topic 1)
_____ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

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

Answer: A

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

NEW QUESTION 142
- (Topic 1)
What is used as a control to detect loss, corruption, or duplication of data?

A. Redundancy check
B. Reasonableness check
C. Hash totals
D. Accuracy check

Answer: C

Explanation:
Hash totals are used as a control to detect loss, corruption, or duplication of datA.

NEW QUESTION 145
- (Topic 1)
Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 147
- (Topic 1)
Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 149
- (Topic 2)
In planning an audit, the MOST critical step is the identification of the:

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

Answer: A

Explanation:

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

NEW QUESTION 153
- (Topic 2)
The extent to which data will be collected during an IS audit should be determined based on the:

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

Answer: D

Explanation:

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

NEW QUESTION 156
- (Topic 2)
While planning an audit, an assessment of risk should be made to provide:

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

Answer: A

Explanation:

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

NEW QUESTION 157
- (Topic 2)
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantifie
B. the auditor wishes to avoid sampling ris
C. generalized audit software is unavailabl
D. the tolerable error rate cannot be determine

Answer: A

Explanation:

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

NEW QUESTION 161
- (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 165
- (Topic 2)
Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

A. The preservation of the chain of custody for electronic evidence
B. Time and cost savings
C. Efficiency and effectiveness
D. Ability to search for violations of intellectual property rights

Answer: A

Explanation:

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

NEW QUESTION 166

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

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

Answer: A

Explanation:

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

NEW QUESTION 171
- (Topic 2)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

A. create the procedures documen
B. terminate the audi
C. conduct compliance testin
D. identify and evaluate existing practice

Answer: D

Explanation:

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

NEW QUESTION 176
- (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 180
- (Topic 2)
Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

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

Answer: C

Explanation:

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

NEW QUESTION 185
- (Topic 2)
The BEST method of proving the accuracy of a system tax calculation is by:

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

D. automatic flowcharting and analysis of the source code of the calculation program

Answer: C

Explanation:

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

NEW QUESTION 187
- (Topic 2)
While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

A. audit trail of the versioning of the work paper
B. approval of the audit phase
C. access rights to the work paper
D. confidentiality of the work paper

Answer: D

Explanation:

Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

NEW QUESTION 190
- (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 192
- (Topic 2)
Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

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

Answer: B

Explanation:

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

NEW QUESTION 195
- (Topic 2)
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

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

Answer: C

Explanation:

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

officer and take on any personal involvement in removing or deleting the unauthorized software.

NEW QUESTION 197
- (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 198
- (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 203
- (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 205
- (Topic 3)
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

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

Answer: C

Explanation:

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

NEW QUESTION 209
- (Topic 3)
The ultimate purpose of IT governance is to:

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

D. centralize control of I

Answer: A

Explanation:

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

NEW QUESTION 211
- (Topic 3)
Responsibility for the governance of IT should rest with the:

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

Answer: D

Explanation:

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

NEW QUESTION 213
- (Topic 3)
A local area network (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 may also be responsible for security administration over the LAN.

NEW QUESTION 216
- (Topic 3)
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual'sexperience and:

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

Answer: D

Explanation:

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

NEW QUESTION 219
- (Topic 3)
An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single perso
B. inadequate succession plannin
C. one person knowing all parts of a syste
D. a disruption of operation

Answer: C

Explanation:

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

NEW QUESTION 222
- (Topic 3)
Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives

Answer: C

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

NEW QUESTION 227
- (Topic 3)
Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

Answer: C

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

NEW QUESTION 229
- (Topic 3)
To support an organization's goals, an IS department should have:

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

Answer: B

Explanation:

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

NEW QUESTION 230
- (Topic 3)
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

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

Answer: C

Explanation:

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

NEW QUESTION 232
- (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 236
- (Topic 3)
A top-down approach to the development of operational policies will help ensure:

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

Answer: A

Explanation:

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

NEW QUESTION 241
- (Topic 3)
When developing a security architecture, which of the following steps should be executed FIRST?

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

Answer: B

Explanation:

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

NEW QUESTION 246
- (Topic 3)
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedure
B. best IT security control practices relevant to a specific entit
C. techniques for securing informatio
D. security polic

Answer: A

Explanation:

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

NEW QUESTION 249
- (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 251
- (Topic 3)
A benefit of open system architecture is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 252
- (Topic 3)
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

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

Answer: A

Explanation:

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

NEW QUESTION 255
- (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 258
- (Topic 3)
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern shouldbe that the:

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

Answer: A

Explanation:

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

NEW QUESTION 260

- (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 263
- (Topic 3)
An IS auditor reviewing the risk assessment process of an organization should FIRST:

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

Answer: C

Explanation:

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

NEW QUESTION 265
- (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 266
- (Topic 3)
The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

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

Answer: B

Explanation:

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

NEW QUESTION 269
- (Topic 3)
An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

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

Answer: A

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

NEW QUESTION 272
- (Topic 3)
Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient service
B. define key performance indicator
C. provide business value to IT project
D. control IT expense

Answer: B

Explanation:

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

NEW QUESTION 275
- (Topic 4)
Which of the following risks could result from inadequate software baselining?

A. Scope creep
B. Sign-off delays
C. Software integrity violations
D. inadequate controls

Answer: A

Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a businesscost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. ChoicesB, C and D may not always result, but choice A is inevitable.

NEW QUESTION 278
- (Topic 4)
The most common reason for the failure of information systems to meet the needs of users is that:

A. user needs are constantly changin
B. the growth of user requirements was forecast inaccuratel
C. the hardware system limits the number of concurrent user
D. user participation in defining the system's requirements was inadequat

Answer: D

Explanation:

Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are, and therefore what the system should accomplish.

NEW QUESTION 283
- (Topic 4)
Change control for business application systems being developed using prototyping could be complicated by the:

A. iterative nature of prototypin
B. rapid pace of modifications in requirements and desig
C. emphasis on reports and screen
D. lack of integrated tool

Answer: B

Explanation:

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

NEW QUESTION 288
- (Topic 4)
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management.

The MOST important concern for an IS auditor is the:

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

Answer: A

Explanation:

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

NEW QUESTION 292
- (Topic 4)
Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

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

Answer: B

Explanation:

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

NEW QUESTION 295
- (Topic 4)
The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

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

Answer: A

Explanation:

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

NEW QUESTION 299
- (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 301
- (Topic 4)
Functional acknowledgements are used:

A. as an audit trail for EDI transaction
B. to functionally describe the IS departmen
C. to document user roles and responsibilitie
D. as a functional description of application softwar

Answer: A

Explanation:

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

NEW QUESTION 306
- (Topic 4)
What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

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

Answer: B

Explanation:

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

NEW QUESTION 307
- (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 308
- (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 311
- (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 312

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

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

Answer: D

Explanation:

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

NEW QUESTION 316
- (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 317
- (Topic 4)
Which of the following is an advantage of the top-down approach to software testing?

A. Interface errors are identified early
B. Testing can be started before all programs are complete
C. it is more effective than other testing approaches
D. Errors in critical modules are detected sooner

Answer: A

Explanation:

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

NEW QUESTION 320
- (Topic 4)
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

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

Answer: B

Explanation:

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

NEW QUESTION 323
- (Topic 4)
An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day

C. implement a source code version control tool
D. Only retest high priority defects

Answer: A

Explanation:

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

NEW QUESTION 326
- (Topic 4)
At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. report the error as a finding and leave further exploration to the auditee's discretio
B. attempt to resolve the erro
C. recommend that problem resolution be escalate
D. ignore the error, as it is not possible to get objective evidence for the software erro

Answer: C

Explanation:

When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

NEW QUESTION 330
- (Topic 4)
From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

A. a big bang deployment after proof of concep
B. prototyping and a one-phase deploymen
C. a deployment plan based on sequenced phase
D. to simulate the new infrastructure before deploymen

Answer: C

Explanation:

When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

NEW QUESTION 333
- (Topic 4)
An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

A. correlation of semantic characteristics of the data migrated between the two system
B. correlation of arithmetic characteristics of the data migrated between the two system
C. correlation of functional characteristics of the processes between the two system
D. relative efficiency of the processes between the two system

Answer: A

Explanation:

Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the data is the same in the new as it was in the old system. Arithmetic characteristics represent aspects of data structure and internal definition in the database, and therefore are less important than the semantic characteristics. A review of the correlation of the functional characteristics or a review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

NEW QUESTION 335
- (Topic 4)
The reason a certification and accreditation process is performed on critical systems is to ensure that:

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

Answer: A

Explanation:

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

NEW QUESTION 336
- (Topic 4)
A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

A. Whether key controls are in place to protect assets and information resources
B. If the system addresses corporate customer requirements
C. Whether the system can meet the performance goals (time and resources)
D. Whether owners have been identified who will be responsible for the process

Answer: A

Explanation:

The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the business process reengineering (BPR) process should achieve, butthey are not the auditor's primary concern.

NEW QUESTION 340
- (Topic 4)
When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

A. systems receiving the output of other system
B. systems sending output to other system
C. systems sending and receiving dat
D. interfaces between the two system

Answer: C

Explanation:

Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

NEW QUESTION 343
- (Topic 4)
An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineerin
B. prototypin
C. software reus
D. reengineerin

Answer: D

Explanation:

Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

NEW QUESTION 345
- (Topic 5)
A benefit of quality of service (QoS) is that the:

A. entire network's availability and performance will be significantly improve
B. telecom carrier will provide the company with accurate service-level compliance report
C. participating applications will have guaranteed service level
D. communications link will be supported by security controls to perform secure online transaction

Answer: C

Explanation:

The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

NEW QUESTION 348
- (Topic 5)
Which of the following will help detect changes made by an intruder to the system log of a server?

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

Answer: B

Explanation:

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

NEW QUESTION 349
- (Topic 5)
The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentialit
B. increased redundanc
C. unauthorized accesse
D. application malfunction

Answer: B

Explanation:

Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional and otherwise unnecessary data handling efforts. Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

NEW QUESTION 350
- (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 353
- (Topic 5)
An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

A. Consistency
B. Isolation
C. Durability
D. Atomicity

Answer: D

Explanation:

Atomicity guarantees that either the entire transaction is processed or none of it is. Consistency ensures that the database is in a legal state when the transaction begins and ends, isolation means that, while in an intermediate state, the transaction data is invisible to external operations. Durability guarantees that a successful transaction will persist, and cannot be undone.

NEW QUESTION 355
- (Topic 5)
An IS auditor finds that client requests were processed multiple times when received
from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

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

Answer: C

Explanation:

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

NEW QUESTION 357
- (Topic 5)
Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

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

Answer: D

Explanation:

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

NEW QUESTION 362
- (Topic 5)
Which of the following is MOST directly affected by network performance monitoring tools?

A. Integrity
B. Availability
C. Completeness
D. Confidentiality

Answer: B

Explanation:

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

NEW QUESTION 364
- (Topic 5)
In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

Answer: C

Explanation:

While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

NEW QUESTION 365
- (Topic 5)
In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

A. application programmer copy the source program and compiled object module to the production librarie
B. application programmer copy the source program to the production libraries and then have the production control group compile the progra
C. production control group compile the object module to the production libraries using the source program in the test environmen

D. production control group copy the source program to the production libraries and then compile the progra

Answer: D

Explanation:

The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

NEW QUESTION 367
- (Topic 5)
The purpose of code signing is to provide assurance that:

A. the software has not been subsequently modifie
B. the application can safely interface with another signed applicatio
C. the signer of the application is truste
D. the private key of the signer has not been compromise

Answer: A

Explanation:

Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

NEW QUESTION 371
- (Topic 5)
An IS auditor should recommend the use of library control software to provide reasonable assurance that:

A. program changes have been authorize
B. only thoroughly tested programs are release
C. modified programs are automatically moved to productio
D. source and executable code integrity is maintaine

Answer: A

Explanation:

Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

NEW QUESTION 376
- (Topic 5)
To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

A. examine the change control system records and trace them forward to object code file
B. review access control permissions operating within the production program librarie
C. examine object code to find instances of changes and trace them back to change control record
D. review change approved designations established within the change control syste

Answer: C

Explanation:

The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes. The other choices are valid procedures to apply in a change control audit but they do not directly address the risk of unauthorized code changes.

NEW QUESTION 380
- (Topic 5)
An IS auditor discovers that developers have operator access to the command line of a
production environment operating system. Which of the following controls wou Id BEST mitigate the risk of undetected and unauthorized program changes to the production
environment?

A. Commands typed on the command line are logged
B. Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs
C. Access to the operating system command line is granted through an access restriction tool with preapproved rights
D. Software development tools and compilers have been removed from the production environment

Answer: B

Explanation:

The matching of hash keys over time would allow detection of changes to files. Choice A is incorrect because having a log is not a control, reviewing the log is a control. Choice C is incorrect because the access was already granted-it does notmatter how. Choice D is wrong because files can be copied to and from the

production environment.

NEW QUESTION 381
- (Topic 5)
Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

A. Change management
B. Backup and recovery
C. incident management
D. Configuration management

Answer: D

Explanation:

The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new release fail, the baseline will provide a point to which to return. The other choices do not provide the processes necessary for establishing software release baselines and are not related to software release baselines.

NEW QUESTION 385
- (Topic 5)
An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration bylT of:

A. the training needs for users after applying the patc
B. any beneficial impact of the patch on the operational system
C. delaying deployment until testing the impact of the patc
D. the necessity of advising end users of new patche

Answer: C

Explanation:

Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

NEW QUESTION 389
- (Topic 5)
Which of the following is a control over component communication failure/errors?

A. Restricting operator access and maintaining audit trails
B. Monitoring and reviewing system engineering activity
C. Providing network redundancy
D. Establishing physical barriers to the data transmitted over the network

Answer: C

Explanation:

Redundancy by building some form of duplication into the network components, such as a link, router or switch to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echochecks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls.

NEW QUESTION 392
- (Topic 5)
In what way is a common gateway interface (CGI) MOST often used on a webserver?

A. Consistent way for transferring data to the application program and back to the user
B. Computer graphics imaging method for movies and TV
C. Graphic user interface for web design
D. interface to access the private gateway domain

Answer: A

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orentering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

NEW QUESTION 395
- (Topic 5)
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

A. Simple Network Management Protocol

B. File Transfer Protocol
C. Simple Mail Transfer Protocol
D. Telnet

Answer: A

Explanation:

The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

NEW QUESTION 398
- (Topic 5)
Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

A. a firewall exist
B. a secure web connection is use
C. the source of the executable file is certai
D. the host web site is part of the organizatio

Answer: C

Explanation:

Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere. It is virtually impossible at thistime to filter at this level. A secure web connection or firewall is considered an external defense. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither asecure web connection nor a firewall can identify an executable file as friendly. Hosting the web site as part of the organization is impractical. Enabling the acceptance of Java applets and/or Active X controls is an all-or-nothing proposition. Theclient will accept the program if the parameters are established to do so.

NEW QUESTION 401
- (Topic 5)
Which of the following types of transmission media provide the BEST security against unauthorized access?

A. Copper wire
B. Twisted pair
C. Fiberoptic cables
D. Coaxial cables

Answer: C

Explanation:

Fiberoptic cables have proven to be more secure than the other mediA. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

NEW QUESTION 406
- (Topic 5)
Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

A. Review the parameter setting
B. Interview the firewall administrato
C. Review the actual procedure
D. Review the device's log file for recent attack

Answer: A

Explanation:

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide audit evidence as strong as choice A.

NEW QUESTION 407
- (Topic 5)
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

A. Simple Object Access Protocol (SOAP)
B. Address Resolution Protocol (ARP)
C. Routing Information Protocol (RIP)
D. Transmission Control Protocol (TCP)

Answer: B

Explanation:

Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform-independent XML-based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connectionand exchange streams of data.

NEW QUESTION 410
- (Topic 5)
Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

A. Session keys are dynamic
B. Private symmetric keys are used
C. Keys are static and shared
D. Source addresses are not encrypted or authenticated

Answer: A

Explanation:

WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy (WEP), which operates with static keys (same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

NEW QUESTION 415
- (Topic 6)
Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

A. System analysis
B. Authorization of access to data
C. Application programming
D. Data administration

Answer: B

Explanation:

The application owner is responsible for authorizing access to datA. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

NEW QUESTION 416
- (Topic 6)
Accountability for the maintenance of appropriate security measures over information assets resides with the:

A. security administrato
B. systems administrato
C. data and systems owner
D. systems operations grou

Answer: C

Explanation:

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

NEW QUESTION 420
- (Topic 6)
An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

A. exposure is greater, since information is available to unauthorized user
B. operating efficiency is enhanced, since anyone can print any report at any tim
C. operating procedures are more effective, since information is easily availabl
D. user friendliness and flexibility is facilitated, since there is a smooth flow of information among user

Answer: A

Explanation:

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

NEW QUESTION 424
- (Topic 6)

The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trai
B. the security administrator has read-only rights to the audit fil
C. date and time stamps are recorded when an action occur
D. users can amend audit trail records when correcting system error

Answer: D

Explanation:

An audit trail is not effective if the details in it can be amended.

NEW QUESTION 426
- (Topic 6)
The implementation of access controls FIRST requires:

A. a classification of IS resource
B. the labeling of IS resource
C. the creation of an access control lis
D. an inventory of IS resource

Answer: D

NEW QUESTION 430
- (Topic 6)
An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

Answer: C

Explanation:

If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' thenit would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

NEW QUESTION 431
- (Topic 6)
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be change
B. passwords are periodically change
C. an automated password management tool be use
D. security awareness training is delivere

Answer: C

Explanation:

The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

NEW QUESTION 434
- (Topic 6)
The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Answer: A

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have theirbadge read at every controlled door no unauthorized person could enter the sensitive areA. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking,but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of

social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

NEW QUESTION 436
- (Topic 6)
Which of the following presents an inherent risk with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

Answer: C

Explanation:

Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the datA. There are only compensatingcontrols for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-re plicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdownof an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which iseffective if there are proper access controls.

NEW QUESTION 440
- (Topic 6)
Which of the following BEST restricts users to those functions needed to perform their duties?

A. Application level access control
B. Data encryption
C. Disabling floppy disk drives
D. Network monitoring device

Answer: A

Explanation:

The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

NEW QUESTION 441
.....

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

Answer: D

Explanation:

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

NEW QUESTION 2
- (Topic 1)
Which of the following is a dynamic analysis tool for the purpose of testing software modules?

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

Answer: A

Explanation:

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

NEW QUESTION 3
- (Topic 1)
Which of the following is a benefit of using callback devices?

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

Answer: A

Explanation:

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

NEW QUESTION 4
- (Topic 1)
A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

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

Answer: A

Explanation:

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

NEW QUESTION 5
- (Topic 1)
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 6
- (Topic 1)
A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

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

Answer: C

Explanation:

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

NEW QUESTION 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)
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 10
- (Topic 1)
Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

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

Answer: A

Explanation:

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

NEW QUESTION 10
- (Topic 1)
A malicious code that changes itself with each file it infects is called a:

A. logic bom
B. stealth viru
C. trojan hors
D. polymorphic viru

Answer: D

Explanation:

A polymorphic virus has the capability of changing its own code, enabling it to have many different variants. Since they have no consistent binary pattern, such viruses are hard to identify.

NEW QUESTION 15
- (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 19
- (Topic 1)
In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

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

Answer: A

Explanation:

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

NEW QUESTION 23
- (Topic 1)
IS auditors are MOST likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 25
- (Topic 1)
A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

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

Answer: C

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

NEW QUESTION 27
- (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 31
- (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 35
- (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 36
- (Topic 1)
Which of the following best characterizes "worms"?

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

Answer: A

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

NEW QUESTION 41
- (Topic 1)
How does the SSL network protocol provide confidentiality?

A. Through symmetric encryption such as RSA
B. Through asymmetric encryption such as Data Encryption Standard, or DES
C. Through asymmetric encryption such as Advanced Encryption Standard, or AES
D. Through symmetric encryption such as Data Encryption Standard, or DES

Answer: D

Explanation:
The SSL protocol provides confidentiality through symmetric encryption such as Data Encryption Standard, or DES.

NEW QUESTION 44
- (Topic 1)
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 48
- (Topic 1)
When is regression testing used to determine whether new application changes have
introduced any errors in the remaining unchanged code?

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

Answer: A

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

NEW QUESTION 50
- (Topic 1)
What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 51
- (Topic 1)
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

Answer: D

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

NEW QUESTION 56
- (Topic 1)
_____ (fill in the blank) is/are are ultimately accountable for the functionality, reliability, and security within IT governance. Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 60
- (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 61
- (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 66
- (Topic 1)
To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 68
- (Topic 1)
Which of the following is best suited for searching for address field duplications?

A. Text search forensic utility software
B. Generalized audit software
C. Productivity audit software
D. Manual review

Answer: B

Explanation:
Generalized audit software can be used to search for address field duplications.

NEW QUESTION 73
- (Topic 1)
An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 75
- (Topic 1)
Who is responsible for implementing cost-effective controls in an automated system?

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

Answer: B

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

NEW QUESTION 80
- (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 81
- (Topic 1)
When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

A. True
B. False

Answer: B

Explanation:
When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered.

NEW QUESTION 86
- (Topic 1)
Who should be responsible for network security operations?

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

Answer: B

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

NEW QUESTION 88
- (Topic 1)
The directory system of a database-management system describes:

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

Answer: B

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

NEW QUESTION 93

- (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 94
- (Topic 1)
What are trojan horse programs? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 95
- (Topic 1)
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

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

Answer: C

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

NEW QUESTION 97
- (Topic 1)
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

A. False
B. True

Answer: B

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

NEW QUESTION 99
- (Topic 1)
What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

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

Answer: C

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

NEW QUESTION 103
- (Topic 1)
What determines the strength of a secret key within a symmetric key cryptosystem?

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

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

Answer: B

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

NEW QUESTION 107
- (Topic 1)
What is often assured through table link verification and reference checks?

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

Answer: A

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

NEW QUESTION 111
- (Topic 1)
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 113
- (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 115
- (Topic 1)
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

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

Answer: B

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

NEW QUESTION 117
- (Topic 1)
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

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

Answer: C

Explanation:

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

NEW QUESTION 120
- (Topic 1)
An IS auditor should carefully review the functional requirements in a systems-development project to ensure that the project is designed to:

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

Answer: A

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

NEW QUESTION 123
- (Topic 1)
When should application controls be considered within the system-development process?

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

Answer: D

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

NEW QUESTION 128
- (Topic 1)
Test and development environments should be separated. True or false?

A. True
B. False

Answer: A

Explanation:
Test and development environments should be separated, to control the stability of the test environment.

NEW QUESTION 132
- (Topic 1)
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 134
- (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 139
- (Topic 1)
_____ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

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

Answer: A

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

NEW QUESTION 142
- (Topic 1)
What is used as a control to detect loss, corruption, or duplication of data?

A. Redundancy check
B. Reasonableness check
C. Hash totals
D. Accuracy check

Answer: C

Explanation:
Hash totals are used as a control to detect loss, corruption, or duplication of datA.

NEW QUESTION 145
- (Topic 1)
Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 147
- (Topic 1)
Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 149
- (Topic 2)
In planning an audit, the MOST critical step is the identification of the:

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

Answer: A

Explanation:

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

NEW QUESTION 153
- (Topic 2)
The extent to which data will be collected during an IS audit should be determined based on the:

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

Answer: D

Explanation:

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

NEW QUESTION 156
- (Topic 2)
While planning an audit, an assessment of risk should be made to provide:

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

Answer: A

Explanation:

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

NEW QUESTION 157
- (Topic 2)
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

A. the probability of error must be objectively quantifie
B. the auditor wishes to avoid sampling ris
C. generalized audit software is unavailabl
D. the tolerable error rate cannot be determine

Answer: A

Explanation:

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

NEW QUESTION 161
- (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 165
- (Topic 2)
Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

A. The preservation of the chain of custody for electronic evidence
B. Time and cost savings
C. Efficiency and effectiveness
D. Ability to search for violations of intellectual property rights

Answer: A

Explanation:

The primary objective of forensic software is to preserve electronic evidence to meet the rules of evidence. Choice B, time and cost savings, and choice C, efficiency and effectiveness, are legitimate concerns that differentiate good from poor forensic software packages. Choice D, the ability to search for intellectual property rights violations, is an example of a use of forensic software.

NEW QUESTION 166

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

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

Answer: A

Explanation:

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

NEW QUESTION 171
- (Topic 2)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

A. create the procedures documen
B. terminate the audi
C. conduct compliance testin
D. identify and evaluate existing practice

Answer: D

Explanation:

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

NEW QUESTION 176
- (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 180
- (Topic 2)
Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

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

Answer: C

Explanation:

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

NEW QUESTION 185
- (Topic 2)
The BEST method of proving the accuracy of a system tax calculation is by:

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

D. automatic flowcharting and analysis of the source code of the calculation program

Answer: C

Explanation:

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

NEW QUESTION 187
- (Topic 2)
While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

A. audit trail of the versioning of the work paper
B. approval of the audit phase
C. access rights to the work paper
D. confidentiality of the work paper

Answer: D

Explanation:

Encryption provides confidentiality for the electronic work papers. Audit trails, audit phase approvals and access to the work papers do not, of themselves, affect the confidentiality but are part of the reason for requiring encryption.

NEW QUESTION 190
- (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 192
- (Topic 2)
Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

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

Answer: B

Explanation:

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

NEW QUESTION 195
- (Topic 2)
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

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

Answer: C

Explanation:

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

officer and take on any personal involvement in removing or deleting the unauthorized software.

NEW QUESTION 197
- (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 198
- (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 203
- (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 205
- (Topic 3)
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

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

Answer: C

Explanation:

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

NEW QUESTION 209
- (Topic 3)
The ultimate purpose of IT governance is to:

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

D. centralize control of I

Answer: A

Explanation:

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

NEW QUESTION 211
- (Topic 3)
Responsibility for the governance of IT should rest with the:

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

Answer: D

Explanation:

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

NEW QUESTION 213
- (Topic 3)
A local area network (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 may also be responsible for security administration over the LAN.

NEW QUESTION 216
- (Topic 3)
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual'sexperience and:

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

Answer: D

Explanation:

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

NEW QUESTION 219
- (Topic 3)
An IS auditor reviewing an organization that uses cross-training practices should assess the risk of:

A. dependency on a single perso
B. inadequate succession plannin
C. one person knowing all parts of a syste
D. a disruption of operation

Answer: C

Explanation:

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

NEW QUESTION 222
- (Topic 3)
Which of the following reduces the potential impact of social engineering attacks?

A. Compliance with regulatory requirements
B. Promoting ethical understanding
C. Security awareness programs
D. Effective performance incentives

Answer: C

Explanation:

Because social engineering is based on deception of the user, the best countermeasure or defense is a security awareness program. The other choices are not user-focused.

NEW QUESTION 227
- (Topic 3)
Which of the following is a risk of cross-training?

A. Increases the dependence on one employee
B. Does not assist in succession planning
C. One employee may know all parts of a system
D. Does not help in achieving a continuity of operations

Answer: C

Explanation:

When cross-training, it would be prudent to first assess the risk of any person knowing all parts of a system and what exposures this may cause. Cross-training has the advantage of decreasing dependence on one employee and, hence, can be part of succession planning. It also provides backup for personnel in the event of absence for any reason and thereby facilitates the continuity of operations.

NEW QUESTION 229
- (Topic 3)
To support an organization's goals, an IS department should have:

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

Answer: B

Explanation:

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

NEW QUESTION 230
- (Topic 3)
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

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

Answer: C

Explanation:

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

NEW QUESTION 232
- (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 236
- (Topic 3)
A top-down approach to the development of operational policies will help ensure:

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

Answer: A

Explanation:

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

NEW QUESTION 241
- (Topic 3)
When developing a security architecture, which of the following steps should be executed FIRST?

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

Answer: B

Explanation:

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

NEW QUESTION 246
- (Topic 3)
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

A. desired result or purpose of implementing specific control procedure
B. best IT security control practices relevant to a specific entit
C. techniques for securing informatio
D. security polic

Answer: A

Explanation:

An IT control objective is defined as the statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. They provide the actual objectives for implementing controls and may or may not be the best practices. Techniques are the means of achieving an objective, and a security policy is a subset of IT control objectives.

NEW QUESTION 249
- (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 251
- (Topic 3)
A benefit of open system architecture is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 252
- (Topic 3)
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

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

Answer: A

Explanation:

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

NEW QUESTION 255
- (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 258
- (Topic 3)
While conducting an audit of a service provider, an IS auditor observes that the service provider has outsourced a part of the work to another provider. Since the work involves confidential information, the IS auditor's PRIMARY concern shouldbe that the:

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

Answer: A

Explanation:

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

NEW QUESTION 260

- (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 263
- (Topic 3)
An IS auditor reviewing the risk assessment process of an organization should FIRST:

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

Answer: C

Explanation:

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

NEW QUESTION 265
- (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 266
- (Topic 3)
The PRIMARY benefit of implementing a security program as part of a security governance framework is the:

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

Answer: B

Explanation:

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

NEW QUESTION 269
- (Topic 3)
An IS auditor who is reviewing incident reports discovers that, in one instance, an important document left on an employee's desk was removed and put in the garbage by the outsourced cleaning staff. Which of the following should the IS auditor recommend to management?

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

Answer: A

Explanation:

An employee leaving an important document on a desk and the cleaning staff removing it may result in a serious impact on the business. Therefore, the IS auditor should recommend that strict controls be implemented by both the organization and the outsourced cleaning agency. That such incidents have not occurred in the past does not reduce the seriousness of their impact. Implementing and monitoring a clear desk policy addresses only one part of the issue. Appropriate confidentiality agreements with the cleaning agency, along with ensuring that the cleaning staff has been educated on the dos and don'ts of the cleaning process, are also controls that should be implemented. The risk here is not a loss of data, but leakage of data to unauthorized sources. A backup policy does not address the issue of unauthorized leakage of information.

NEW QUESTION 272
- (Topic 3)
Before implementing an IT balanced scorecard, an organization must:

A. deliver effective and efficient service
B. define key performance indicator
C. provide business value to IT project
D. control IT expense

Answer: B

Explanation:

A definition of key performance indicators is required before implementing an IT balanced scorecard. Choices A, C and D are objectives.

NEW QUESTION 275
- (Topic 4)
Which of the following risks could result from inadequate software baselining?

A. Scope creep
B. Sign-off delays
C. Software integrity violations
D. inadequate controls

Answer: A

Explanation:

A software baseline is the cut-off point in the design and development of a system beyond which additional requirements or modifications to the design do not or cannot occur without undergoing formal strict procedures for approval based on a businesscost-benefit analysis. Failure to adequately manage the requirements of a system through baselining can result in a number of risks. Foremost among these risks is scope creep, the process through which requirements change during development. ChoicesB, C and D may not always result, but choice A is inevitable.

NEW QUESTION 278
- (Topic 4)
The most common reason for the failure of information systems to meet the needs of users is that:

A. user needs are constantly changin
B. the growth of user requirements was forecast inaccuratel
C. the hardware system limits the number of concurrent user
D. user participation in defining the system's requirements was inadequat

Answer: D

Explanation:

Lack of adequate user involvement, especially in the system's requirements phase, will usually result in a system that does not fully or adequately address the needs of the user. Only users can define what their needs are, and therefore what the system should accomplish.

NEW QUESTION 283
- (Topic 4)
Change control for business application systems being developed using prototyping could be complicated by the:

A. iterative nature of prototypin
B. rapid pace of modifications in requirements and desig
C. emphasis on reports and screen
D. lack of integrated tool

Answer: B

Explanation:

Changes in requirements and design happen so quickly that they are seldom documented or approved. Choices A, C and D are characteristics of prototyping, but they do not have an adverse effect on change control.

NEW QUESTION 288
- (Topic 4)
While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management.

The MOST important concern for an IS auditor is the:

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

Answer: A

Explanation:

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

NEW QUESTION 292
- (Topic 4)
Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

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

Answer: B

Explanation:

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

NEW QUESTION 295
- (Topic 4)
The purpose of a checksum on an amount field in an electronic data interchange (EDI) communication of financial transactions is to ensure:

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

Answer: A

Explanation:

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

NEW QUESTION 299
- (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 301
- (Topic 4)
Functional acknowledgements are used:

A. as an audit trail for EDI transaction
B. to functionally describe the IS departmen
C. to document user roles and responsibilitie
D. as a functional description of application softwar

Answer: A

Explanation:

Functional acknowledgements are standard EDI transactions that tell trading partners that their electronic documents were received. Different types of functional acknowledgments provide various levels of detail and, therefore, can act as an audit trail for EDI transactions. The other choices are not relevant to the description of functional acknowledgements.

NEW QUESTION 306
- (Topic 4)
What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

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

Answer: B

Explanation:

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

NEW QUESTION 307
- (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 308
- (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 311
- (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 312

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

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

Answer: D

Explanation:

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

NEW QUESTION 316
- (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 317
- (Topic 4)
Which of the following is an advantage of the top-down approach to software testing?

A. Interface errors are identified early
B. Testing can be started before all programs are complete
C. it is more effective than other testing approaches
D. Errors in critical modules are detected sooner

Answer: A

Explanation:

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

NEW QUESTION 320
- (Topic 4)
Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

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

Answer: B

Explanation:

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

NEW QUESTION 323
- (Topic 4)
An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day

C. implement a source code version control tool
D. Only retest high priority defects

Answer: A

Explanation:

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

NEW QUESTION 326
- (Topic 4)
At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

A. report the error as a finding and leave further exploration to the auditee's discretio
B. attempt to resolve the erro
C. recommend that problem resolution be escalate
D. ignore the error, as it is not possible to get objective evidence for the software erro

Answer: C

Explanation:

When an IS auditor observes such conditions, it is best to fully apprise the auditee and suggest that further problem resolutions be attempted. Recording it as a minor error and leaving it to the auditee's discretion would be inappropriate, and neglecting the error would indicate that the auditor has not taken steps to further probe the issue to its logical end.

NEW QUESTION 330
- (Topic 4)
From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

A. a big bang deployment after proof of concep
B. prototyping and a one-phase deploymen
C. a deployment plan based on sequenced phase
D. to simulate the new infrastructure before deploymen

Answer: C

Explanation:

When developing a large and complex IT infrastructure, the best practice is to use a phased approach to fitting the entire system together. This will provide greater assurance of quality results. The other choices are riskier approaches.

NEW QUESTION 333
- (Topic 4)
An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:

A. correlation of semantic characteristics of the data migrated between the two system
B. correlation of arithmetic characteristics of the data migrated between the two system
C. correlation of functional characteristics of the processes between the two system
D. relative efficiency of the processes between the two system

Answer: A

Explanation:

Due to the fact that the two systems could have a different data representation, including the database schema, the IS auditor's main concern should be to verify that the interpretation of the data is the same in the new as it was in the old system. Arithmetic characteristics represent aspects of data structure and internal definition in the database, and therefore are less important than the semantic characteristics. A review of the correlation of the functional characteristics or a review of the relative efficiencies of the processes between the two systems is not relevant to a data migration review.

NEW QUESTION 335
- (Topic 4)
The reason a certification and accreditation process is performed on critical systems is to ensure that:

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

Answer: A

Explanation:

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

NEW QUESTION 336
- (Topic 4)
A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

A. Whether key controls are in place to protect assets and information resources
B. If the system addresses corporate customer requirements
C. Whether the system can meet the performance goals (time and resources)
D. Whether owners have been identified who will be responsible for the process

Answer: A

Explanation:

The audit team must advocate the inclusion of the key controls and verify that the controls are in place before implementing the new process. Choices B, C and D are objectives that the business process reengineering (BPR) process should achieve, butthey are not the auditor's primary concern.

NEW QUESTION 340
- (Topic 4)
When two or more systems are integrated, input/output controls must be reviewed by an IS auditor in the:

A. systems receiving the output of other system
B. systems sending output to other system
C. systems sending and receiving dat
D. interfaces between the two system

Answer: C

Explanation:

Both of the systems must be reviewed for input/output controls, since the output for one system is the input for the other.

NEW QUESTION 343
- (Topic 4)
An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

A. reverse engineerin
B. prototypin
C. software reus
D. reengineerin

Answer: D

Explanation:

Old (legacy) systems that have been corrected, adapted and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing and using previously developed software components. The reusable components are integrated into the current software product systematically.

NEW QUESTION 345
- (Topic 5)
A benefit of quality of service (QoS) is that the:

A. entire network's availability and performance will be significantly improve
B. telecom carrier will provide the company with accurate service-level compliance report
C. participating applications will have guaranteed service level
D. communications link will be supported by security controls to perform secure online transaction

Answer: C

Explanation:

The main function of QoS is to optimize network performance by assigning priority to business applications and end users, through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools and others, the tool itself is not intended to provide security controls.

NEW QUESTION 348
- (Topic 5)
Which of the following will help detect changes made by an intruder to the system log of a server?

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

Answer: B

Explanation:

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

NEW QUESTION 349
- (Topic 5)
The database administrator (DBA) suggests that DB efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentialit
B. increased redundanc
C. unauthorized accesse
D. application malfunction

Answer: B

Explanation:

Normalization is a design or optimization process for a relational database (DB) that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy which is usually considered positive when it is a question of resource availability is negative in a database environment, since it demands additional and otherwise unnecessary data handling efforts. Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses or application malfunctions.

NEW QUESTION 350
- (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 353
- (Topic 5)
An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error, and are not rolled back. Which of the following transaction processing features has been violated?

A. Consistency
B. Isolation
C. Durability
D. Atomicity

Answer: D

Explanation:

Atomicity guarantees that either the entire transaction is processed or none of it is. Consistency ensures that the database is in a legal state when the transaction begins and ends, isolation means that, while in an intermediate state, the transaction data is invisible to external operations. Durability guarantees that a successful transaction will persist, and cannot be undone.

NEW QUESTION 355
- (Topic 5)
An IS auditor finds that client requests were processed multiple times when received
from different independent departmental databases, which are synchronized weekly. What would be the BEST recommendation?

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

Answer: C

Explanation:

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

NEW QUESTION 357
- (Topic 5)
Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?

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

Answer: D

Explanation:

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

NEW QUESTION 362
- (Topic 5)
Which of the following is MOST directly affected by network performance monitoring tools?

A. Integrity
B. Availability
C. Completeness
D. Confidentiality

Answer: B

Explanation:

In case of a disruption in service, one of the key functions of network performance monitoring tools is to ensure that the information has remained unaltered. It is a function of security monitoring to assure confidentiality by using such tools as encryption. However, the most important aspect of network performance is assuring the ongoing dependence on connectivity to run the business. Therefore, the characteristic that benefits the most from network monitoring is availability.

NEW QUESTION 364
- (Topic 5)
In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?

A. Automated logging of changes to development libraries
B. Additional staff to provide separation of duties
C. Procedures that verify that only approved program changes are implemented
D. Access controls to prevent the operator from making program modifications

Answer: C

Explanation:

While it would be preferred that strict separation of duties be adhered to and that additional staff is recruited as suggested in choice B, this practice is not always possible in small organizations. An IS auditor must look at recommended alternative processes. Of the choices, C is the only practical one that has an impact. An IS auditor should recommend processes that detect changes to production source and object code, such as code comparisons, so the changes can be reviewed on a regular basis by a third party. This would be a compensating control process. Choice A, involving logging of changes to development libraries, would not detect changes to production libraries. Choice D is in effect requiring a third party to do the changes, which may not be practical in a small organization.

NEW QUESTION 365
- (Topic 5)
In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:

A. application programmer copy the source program and compiled object module to the production librarie
B. application programmer copy the source program to the production libraries and then have the production control group compile the progra
C. production control group compile the object module to the production libraries using the source program in the test environmen

D. production control group copy the source program to the production libraries and then compile the progra

Answer: D

Explanation:

The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program.

NEW QUESTION 367
- (Topic 5)
The purpose of code signing is to provide assurance that:

A. the software has not been subsequently modifie
B. the application can safely interface with another signed applicatio
C. the signer of the application is truste
D. the private key of the signer has not been compromise

Answer: A

Explanation:

Code signing can only ensure that the executable code has not been modified after being signed. The other choices are incorrect and actually represent potential and exploitable weaknesses of code signing.

NEW QUESTION 371
- (Topic 5)
An IS auditor should recommend the use of library control software to provide reasonable assurance that:

A. program changes have been authorize
B. only thoroughly tested programs are release
C. modified programs are automatically moved to productio
D. source and executable code integrity is maintaine

Answer: A

Explanation:

Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized. Library control software is concerned with authorized program changes and would not automatically move modified programs into production and cannot determine whether programs have been thoroughly tested. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. However, subsequent events such as a hardware failure can result in a lack of consistency between source and executable code.

NEW QUESTION 376
- (Topic 5)
To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

A. examine the change control system records and trace them forward to object code file
B. review access control permissions operating within the production program librarie
C. examine object code to find instances of changes and trace them back to change control record
D. review change approved designations established within the change control syste

Answer: C

Explanation:

The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes. The other choices are valid procedures to apply in a change control audit but they do not directly address the risk of unauthorized code changes.

NEW QUESTION 380
- (Topic 5)
An IS auditor discovers that developers have operator access to the command line of a
production environment operating system. Which of the following controls wou Id BEST mitigate the risk of undetected and unauthorized program changes to the production
environment?

A. Commands typed on the command line are logged
B. Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs
C. Access to the operating system command line is granted through an access restriction tool with preapproved rights
D. Software development tools and compilers have been removed from the production environment

Answer: B

Explanation:

The matching of hash keys over time would allow detection of changes to files. Choice A is incorrect because having a log is not a control, reviewing the log is a control. Choice C is incorrect because the access was already granted-it does notmatter how. Choice D is wrong because files can be copied to and from the

production environment.

NEW QUESTION 381
- (Topic 5)
Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

A. Change management
B. Backup and recovery
C. incident management
D. Configuration management

Answer: D

Explanation:

The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new release fail, the baseline will provide a point to which to return. The other choices do not provide the processes necessary for establishing software release baselines and are not related to software release baselines.

NEW QUESTION 385
- (Topic 5)
An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration bylT of:

A. the training needs for users after applying the patc
B. any beneficial impact of the patch on the operational system
C. delaying deployment until testing the impact of the patc
D. the necessity of advising end users of new patche

Answer: C

Explanation:

Deploying patches without testing exposes an organization to the risk of system disruption or failure. Normally, there is no need for training or advising users when a new operating system patch has been installed. Any beneficial impact is less important than the risk of unavailability that could be avoided with proper testing.

NEW QUESTION 389
- (Topic 5)
Which of the following is a control over component communication failure/errors?

A. Restricting operator access and maintaining audit trails
B. Monitoring and reviewing system engineering activity
C. Providing network redundancy
D. Establishing physical barriers to the data transmitted over the network

Answer: C

Explanation:

Redundancy by building some form of duplication into the network components, such as a link, router or switch to prevent loss, delays or data duplication is a control over component communication failure or error. Other related controls are loop/echochecks to detect line errors, parity checks, error correction codes and sequence checks. Choices A, B and D are communication network controls.

NEW QUESTION 392
- (Topic 5)
In what way is a common gateway interface (CGI) MOST often used on a webserver?

A. Consistent way for transferring data to the application program and back to the user
B. Computer graphics imaging method for movies and TV
C. Graphic user interface for web design
D. interface to access the private gateway domain

Answer: A

Explanation:

The common gateway interface (CGI) is a standard way for a web server to pass a user's request to an application program and to move data back and forth to the user. When the user requests a web page (for example, by clicking on a highlighted word orentering a web site address), the server sends back the requested page. However, when a user fills out a form on a web page and submits it, it usually needs to be processed by an application program. The web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method, or convention, for passing data back and forth between the server and the application is called the common gateway interface (CGI). It is part of the web's HTTP protocol.

NEW QUESTION 395
- (Topic 5)
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

A. Simple Network Management Protocol

B. File Transfer Protocol
C. Simple Mail Transfer Protocol
D. Telnet

Answer: A

Explanation:

The Simple Network Management Protocol provides a means to monitor and control network devices and to manage configurations and performance. The File Transfer Protocol (FTP) transfers files from a computer on the Internet to the user's computer and does not have any functionality related to monitoring network devices. Simple Mail Transfer Protocol (SMTP) is a protocol for sending and receiving e-mail messages and does not provide any monitoring or management for network devices. Telnet is a standard terminal emulation protocol used for remote terminal connections, enabling users to log into remote systems and use resources as if they were connected to a local system; it does not provide any monitoring or management of network devices.

NEW QUESTION 398
- (Topic 5)
Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

A. a firewall exist
B. a secure web connection is use
C. the source of the executable file is certai
D. the host web site is part of the organizatio

Answer: C

Explanation:

Acceptance of these mechanisms should be based on established trust. The control is provided by only knowing the source and then allowing the acceptance of the applets. Hostile applets can be received from anywhere. It is virtually impossible at thistime to filter at this level. A secure web connection or firewall is considered an external defense. A firewall will find it more difficult to filter a specific file from a trusted source. A secure web connection provides confidentiality. Neither asecure web connection nor a firewall can identify an executable file as friendly. Hosting the web site as part of the organization is impractical. Enabling the acceptance of Java applets and/or Active X controls is an all-or-nothing proposition. Theclient will accept the program if the parameters are established to do so.

NEW QUESTION 401
- (Topic 5)
Which of the following types of transmission media provide the BEST security against unauthorized access?

A. Copper wire
B. Twisted pair
C. Fiberoptic cables
D. Coaxial cables

Answer: C

Explanation:

Fiberoptic cables have proven to be more secure than the other mediA. Satellite transmission and copper wire can be violated with inexpensive equipment. Coaxial cable can also be violated more easily than other transmission media.

NEW QUESTION 406
- (Topic 5)
Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

A. Review the parameter setting
B. Interview the firewall administrato
C. Review the actual procedure
D. Review the device's log file for recent attack

Answer: A

Explanation:

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide audit evidence documentation. The other choices do not provide audit evidence as strong as choice A.

NEW QUESTION 407
- (Topic 5)
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

A. Simple Object Access Protocol (SOAP)
B. Address Resolution Protocol (ARP)
C. Routing Information Protocol (RIP)
D. Transmission Control Protocol (TCP)

Answer: B

Explanation:

Address Resolution Protocol (ARP) provides dynamic address mapping between an IP address and hardware address. Simple Object Access Protocol (SOAP) is a platform-independent XML-based protocol, enabling applications to communicate with each other over the Internet, and does not deal with media access control (MAC) addresses. Routing Information Protocol (RIP) specifies how routers exchange routing table information. Transmission Control Protocol (TCP) enables two hosts to establish a connectionand exchange streams of data.

NEW QUESTION 410
- (Topic 5)
Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

A. Session keys are dynamic
B. Private symmetric keys are used
C. Keys are static and shared
D. Source addresses are not encrypted or authenticated

Answer: A

Explanation:

WPA uses dynamic session keys, achieving stronger encryption than wireless encryption privacy (WEP), which operates with static keys (same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

NEW QUESTION 415
- (Topic 6)
Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

A. System analysis
B. Authorization of access to data
C. Application programming
D. Data administration

Answer: B

Explanation:

The application owner is responsible for authorizing access to datA. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

NEW QUESTION 416
- (Topic 6)
Accountability for the maintenance of appropriate security measures over information assets resides with the:

A. security administrato
B. systems administrato
C. data and systems owner
D. systems operations grou

Answer: C

Explanation:

Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

NEW QUESTION 420
- (Topic 6)
An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:

A. exposure is greater, since information is available to unauthorized user
B. operating efficiency is enhanced, since anyone can print any report at any tim
C. operating procedures are more effective, since information is easily availabl
D. user friendliness and flexibility is facilitated, since there is a smooth flow of information among user

Answer: A

Explanation:

Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

NEW QUESTION 424
- (Topic 6)

The reliability of an application system's audit trail may be questionable if:

A. user IDs are recorded in the audit trai
B. the security administrator has read-only rights to the audit fil
C. date and time stamps are recorded when an action occur
D. users can amend audit trail records when correcting system error

Answer: D

Explanation:

An audit trail is not effective if the details in it can be amended.

NEW QUESTION 426
- (Topic 6)
The implementation of access controls FIRST requires:

A. a classification of IS resource
B. the labeling of IS resource
C. the creation of an access control lis
D. an inventory of IS resource

Answer: D

NEW QUESTION 430
- (Topic 6)
An information security policy stating that 'the display of passwords must be masked or suppressed' addresses which of the following attack methods?

A. Piggybacking
B. Dumpster diving
C. Shoulder surfing
D. Impersonation

Answer: C

Explanation:

If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to 'the display of passwords.' If the policy referred to 'the display and printing of passwords' thenit would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information), impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

NEW QUESTION 431
- (Topic 6)
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

A. the company policy be change
B. passwords are periodically change
C. an automated password management tool be use
D. security awareness training is delivere

Answer: C

Explanation:

The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and would enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period of time. Choices A, B and D do not enforce compliance.

NEW QUESTION 434
- (Topic 6)
The information security policy that states 'each individual must have their badge read at every controlled door' addresses which of the following attack methods?

A. Piggybacking
B. Shoulder surfing
C. Dumpster diving
D. Impersonation

Answer: A

Explanation:

Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger, if every employee must have theirbadge read at every controlled door no unauthorized person could enter the sensitive areA. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking,but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee, trying to retrieve the desired information. Some forms of

social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

NEW QUESTION 436
- (Topic 6)
Which of the following presents an inherent risk with no distinct identifiable preventive controls?

A. Piggybacking
B. Viruses
C. Data diddling
D. Unauthorized application shutdown

Answer: C

Explanation:

Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses, because it requires limited technical knowledge and occurs before computer security can protect the datA. There are only compensatingcontrols for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-re plicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdownof an application can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which iseffective if there are proper access controls.

NEW QUESTION 440
- (Topic 6)
Which of the following BEST restricts users to those functions needed to perform their duties?

A. Application level access control
B. Data encryption
C. Disabling floppy disk drives
D. Network monitoring device

Answer: A

Explanation:

The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

NEW QUESTION 441
.....

Relate Links

100% Pass Your CISA Exam with Exambible Prep Materials

https://www.exambible.com/CISA-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/