Exam Questions CISA

Isaca CISA

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

NEW QUESTION 1
- (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 2
- (Topic 1)
Which of the following data validation edits is effective in detecting transposition and transcription errors?

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

Answer: B

Explanation:

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

NEW QUESTION 3
- (Topic 1)
In an EDI process, the device which transmits and receives electronic documents is the:

A. communications handle
B. EDI translato
C. application interfac
D. EDI interfac

Answer: A

Explanation:

A communications handler transmits and receives electronic documents between trading partners and/or wide area networks (WANs).

NEW QUESTION 4
- (Topic 1)
The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

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

Answer: D

Explanation:

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

NEW QUESTION 5
- (Topic 1)
A data administrator is responsible for:

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

Answer: B

Explanation:

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

NEW QUESTION 6
- (Topic 1)
A database administrator is responsible for:

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

Answer: C

Explanation:

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

NEW QUESTION 7
- (Topic 1)
An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

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

Answer: D

Explanation:

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

NEW QUESTION 8
- (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 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)
An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST costeffective test of the DRP?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

Answer: B

Explanation:

A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for the disaster recovery.

NEW QUESTION 12
- (Topic 1)
Which of the following is a data validation edit and control?

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

Answer: B

Explanation:

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

NEW QUESTION 13
- (Topic 1)
What type of approach to the development of organizational policies is often driven by risk assessment?

A. Bottom-up
B. Top-down
C. Comprehensive
D. Integrated

Answer: B

Explanation:
A bottom-up approach to the development of organizational policies is often driven by risk assessment.

NEW QUESTION 17
- (Topic 1)
Which of the following could lead to an unintentional loss of confidentiality? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 21
- (Topic 1)
What is the most common purpose of a virtual private network implementation?

A. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such

as the Interne
B. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a dedicated T1 connectio
C. A virtual private network (VPN) helps to secure access within an enterprise when communicating over a dedicated T1 connection between network segments within the same facilit
D. A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over a wireless connectio

Answer: A

Explanation:
A virtual private network (VPN) helps to secure access between an enterprise and its partners when communicating over an otherwise unsecured channel such as the Internet.

NEW QUESTION 23
- (Topic 1)
What can be very helpful to an IS auditor when determining the efficacy of a systems maintenance program? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 24
- (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 28
- (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 32
- (Topic 1)
Which of the following provides the strongest authentication for physical access control?

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

Answer: D

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

NEW QUESTION 34
- (Topic 1)
Who is ultimately responsible and accountable for reviewing user access to systems?

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

Answer: C

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

NEW QUESTION 38
- (Topic 1)
Establishing data ownership is an important first step for which of the following processes? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 39
- (Topic 1)
Which of the following typically focuses on making alternative processes and resources available for transaction processing?

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

Answer: D

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

NEW QUESTION 43
- (Topic 1)
Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

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

Answer: C

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

NEW QUESTION 45
- (Topic 1)
What influences decisions regarding criticality of assets?

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

Answer: C

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

NEW QUESTION 46
- (Topic 1)
Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

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

Answer: A

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

NEW QUESTION 51
- (Topic 1)
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive
management, such as the _____. (fill-in-the-blank)

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

Answer: C

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

NEW QUESTION 52
- (Topic 1)
Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 55
- (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 58
- (Topic 1)
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

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

Answer: B

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

NEW QUESTION 60
- (Topic 1)
What often results in project scope creep when functional requirements are not defined as well as they could be?

A. Inadequate software baselining
B. Insufficient strategic planning
C. Inaccurate resource allocation
D. Project delays

Answer: A

Explanation:
Inadequate software baselining often results in project scope creep because functional requirements are not defined as well as they could be.

NEW QUESTION 63
- (Topic 1)
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any

intensive data-calculation procedures. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 68
- (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 69
- (Topic 1)
What can be used to help identify and investigate unauthorized transactions? Choose the BEST answer.

A. Postmortem review
B. Reasonableness checks
C. Data-mining techniques
D. Expert systems

Answer: C

Explanation:
Data-mining techniques can be used to help identify and investigate unauthorized transactions.

NEW QUESTION 73
- (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 75
- (Topic 1)
A check digit is an effective edit check to:

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

Answer: B

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

NEW QUESTION 78
- (Topic 1)
Which of the following is the MOST critical step in planning an audit?

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

Answer: C

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

NEW QUESTION 79
- (Topic 1)
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 84
- (Topic 1)
What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 85
- (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 87
- (Topic 1)
How is the risk of improper file access affected upon implementing a database system?

A. Risk varie
B. Risk is reduce
C. Risk is not affecte
D. Risk is increase

Answer: D

Explanation:
Improper file access becomes a greater risk when implementing a database system.

NEW QUESTION 90
- (Topic 1)
In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

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

Answer: B

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

NEW QUESTION 95

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

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

Answer: A

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

NEW QUESTION 98
- (Topic 1)
What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

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

Answer: C

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

NEW QUESTION 103
- (Topic 1)
What is a common vulnerability, allowing denial-of-service attacks?

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

Answer: C

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

NEW QUESTION 106
- (Topic 1)
What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

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

Answer: A

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

NEW QUESTION 109
- (Topic 1)
What process is used to validate a subject's identity?

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

Answer: D

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

NEW QUESTION 110
- (Topic 1)
Using the OSI reference model, what layer(s) is/are used to encrypt data?

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

Answer: C

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

NEW QUESTION 111
- (Topic 1)
Which of the following is the most fundamental step in preventing virus attacks?

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

Answer: A

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

NEW QUESTION 112
- (Topic 1)
Why is a clause for requiring source code escrow in an application vendor agreement important?

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

Answer: D

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

NEW QUESTION 117
- (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 119
- (Topic 1)
What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 124
- (Topic 1)
Who is responsible for the overall direction, costs, and timetables for systems-development projects?

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

Answer: B

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

NEW QUESTION 126
- (Topic 1)
Input/output controls should be implemented for which applications in an integrated systems environment?

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

Answer: C

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

NEW QUESTION 130
- (Topic 1)
What is the primary security concern for EDI environments? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 133
- (Topic 1)
Business process re-engineering often results in _____ automation, which results in _____ number of people using technology. Fill in the blanks.

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

Answer: A

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

NEW QUESTION 136
- (Topic 1)
Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 140
- (Topic 1)
An IS auditor is using a statistical sample to inventory the tape library. What type of test would this be considered?

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

Answer: A

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

NEW QUESTION 145
- (Topic 2)
The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

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

Answer: B

Explanation:

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

NEW QUESTION 150
- (Topic 2)
Which of the following is a substantive test?

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

Answer: C

Explanation:

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

NEW QUESTION 151
- (Topic 2)
Which of the following is a benefit of a risk-based approach to audit planning? Audit:

A. scheduling may be performed months in advanc
B. budgets are more likely to be met by the IS audit staf
C. staff will be exposed to a variety of technologie
D. resources are allocated to the areas of highest concern

Answer: D

Explanation:

The risk-based approach is designed to ensure audit time is spent on the areas of highest risk. The development of an audit schedule is not addressed by a risk-based approach. Audit schedules may be prepared months in advance using various schedulingmethods. A risk approach does not have a direct correlation to the audit staff meeting time budgets on a particular audit, nor does it necessarily mean a wider variety of audits will be performed in a given year.

NEW QUESTION 155
- (Topic 2)
During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

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

Answer: A

Explanation:

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

NEW QUESTION 160
- (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
CORRECT TEXT - (Topic 2)
The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

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

Answer: B

NEW QUESTION 168
- (Topic 2)
In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 172
- (Topic 2)
During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

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

Answer: C

Explanation:

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

NEW QUESTION 177
- (Topic 2)
An integrated test facility is considered a useful audit tool because it:

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

Answer: C

Explanation:

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

NEW QUESTION 178
- (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 180
- (Topic 2)
In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

A. Testing whether inappropriate personnel can change application parameters
B. Tracing purchase orders to a computer listing
C. Comparing receiving reports to purchase order details
D. Reviewing the application documentation

Answer: A

Explanation:

To determine purchase order validity, testing access controls will provide the best evidence. Choices B and C are based on after-the-fact approaches, while choice D does not serve the purpose because what is in the system documentation may not be thesame as what is happening.

NEW QUESTION 183
- (Topic 2)
Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

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

Answer: C

Explanation:

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

NEW QUESTION 187
- (Topic 2)
During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

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

Answer: B

Explanation:

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

NEW QUESTION 191
- (Topic 2)
The final decision to include a material finding in an audit report should be made by the:

A. audit committe
B. auditee's manage
C. IS audito
D. CEO of the organization

Answer: C

Explanation:

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

auditor.

NEW QUESTION 195
- (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 199
- (Topic 3)
When implementing an IT governance framework in an organization the MOST important objective is:

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

Answer: A

Explanation:

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

NEW QUESTION 202
- (Topic 3)
An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

A. User acceptance testing (UAT) occur for all reports before release into production
B. Organizational data governance practices be put in place
C. Standard software tools be used for report development
D. Management sign-off on requirements for new reports

Answer: B

Explanation:

This choice directly addresses the problem. An organizationwide approach is needed to achieve effective management of data assets. This includes enforcing standard definitions of data elements, which is part of a data governance initiative. The otherchoices, while sound development practices, do not address the root cause of the problem described.

NEW QUESTION 203
- (Topic 3)
From a control perspective, the key element in job descriptions is that they:

A. provide instructions on how to do the job and define authorit
B. are current, documented and readily available to the employe
C. communicate management's specific job performance expectation
D. establish responsibility and accountability for the employee's action

Answer: D

Explanation:

From a control perspective, a job description should establish responsibility and accountability. This will aid in ensuring that users are given system access in accordance with their defined job responsibilities. The other choices are not directly related to controls. Providing instructions on how to do the job and defining authority addresses the managerial and procedural aspects of the job. It is important that job descriptions are current, documented and readily available to the employee, but this in itself is not a control. Communication of management's specific expectations for job performance outlines the standard of performance and would not necessarily include controls.

NEW QUESTION 205
- (Topic 3)
Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

A. ensure the employee maintains a good quality of life, which will lead to greater productivit
B. reduce the opportunity for an employee to commit an improper or illegal ac

C. provide proper cross-training for another employe
D. eliminate the potential disruption caused when an employee takes vacation one day at a tim

Answer: B

Explanation:

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

NEW QUESTION 210
- (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 213
- (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 215
- (Topic 3)
In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

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

Answer: A

Explanation:

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

NEW QUESTION 219
- (Topic 3)
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

A. has been approved by line managemen
B. does not vary from the IS department's preliminary budge
C. complies with procurement procedure
D. supports the business objectives of the organizatio

Answer: D

Explanation:

Strategic planning sets corporate or department objectives into motion. Both long-term and short-term strategic plans should be consistent with the organization's broader plans and business objectives for attaining these goals. Choice A is incorrectsince line management prepared the plans.

NEW QUESTION 222
- (Topic 3)
When reviewing IS strategies, an IS auditor can BEST assess whether IS strategy supports the organizations' business objectives by determining if IS:

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

Answer: B

Explanation:

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

NEW QUESTION 227
- (Topic 3)
Which of the following should be included in an organization's IS security policy?

A. A list of key IT resources to be secured
B. The basis for access authorization
C. Identity of sensitive security features
D. Relevant software security features

Answer: B

Explanation:

The security policy provides the broad framework of security, as laid down and approved by senior management. It includes a definition of those authorized to grant access and the basis for granting the access. Choices A, B and C are more detailed than that which should be included in a policy.

NEW QUESTION 230
- (Topic 3)
The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

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

Answer: D

Explanation:

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

NEW QUESTION 234
- (Topic 3)
In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

A. implementatio
B. complianc
C. documentatio
D. sufficienc

Answer: D

Explanation:

An IS auditor should first evaluate the definition of the minimum baseline level by ensuring the sufficiency of controls. Documentation, implementation and compliance are further steps.

NEW QUESTION 235
- (Topic 3)
An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

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

Answer: C

Explanation:

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

NEW QUESTION 240
- (Topic 3)
An example of a direct benefit to be derived from a proposed IT-related business investment is:

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

Answer: D

Explanation:

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

NEW QUESTION 245
- (Topic 3)
In the context of effective information security governance, the primary objective of value delivery is to:

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

Answer: A

Explanation:

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

NEW QUESTION 247
- (Topic 3)
A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

A. compute the amortization of the related asset
B. calculate a return on investment (ROI).
C. apply a qualitative approac
D. spend the time needed to define exactly the loss amoun

Answer: C

Explanation:

The common practice, when it is difficult to calculate the financial losses, is to take a qualitative approach, in which the manager affected by the risk defines the financial loss in terms of a weighted factor {e.g., one is a very low impact to thebusiness and five is a very high impact). An ROI is computed when there is predictable savings or revenues that can be compared to the investment needed to realize the revenues. Amortization is used in a profit and loss statement, not in computing potential losses. Spending the time needed to define exactly the total amount is normally a wrong approach. If it has been difficult to estimate potential losses (e.g., losses derived from erosion of public image due to a hack attack), that situation is not likely to change, and at the end of the day, the result will be a not well-supported evaluation.

NEW QUESTION 251
- (Topic 3)
Assessing IT risks is BEST achieved by:

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

Answer: A

Explanation:

To assess IT risks, threats and vulnerabilities need to be evaluated using qualitative or quantitative risk assessment approaches. Choices B, C and D are potentially useful inputs to the risk assessment process, but by themselves are not sufficient.Basing an assessment on past losses will not adequately reflect inevitable changes to the firm's IT assets, projects, controls and strategic environment. There are also likely to be problems with the scope and quality of the loss data available to beassessed. Comparable organizations will have differences in their IT assets, control environment and strategic circumstances. Therefore, their

loss experience cannot be used to directly assess organizational IT risk. Control weaknesses identified during audits will be relevant in assessing threat exposure and further analysis may be needed to assess threat probability. Depending on the scope of the audit coverage, it is possible that not all of the critical IT assets and projects will have recently been audited, and there may not be a sufficient assessment of strategic IT risks.

NEW QUESTION 255
- (Topic 3)
Which of the following should be considered FIRST when implementing a risk management program?

A. An understanding of the organization's threat, vulnerability and risk profile
B. An understanding of the risk exposures and the potential consequences of compromise
C. A determination of risk management priorities based on potential consequences
D. A risk mitigation strategy sufficient to keep risk consequences at an acceptable level

Answer: A

Explanation:

Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

NEW QUESTION 256
- (Topic 3)
As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

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

Answer: A

Explanation:

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

NEW QUESTION 258
- (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 262
- (Topic 4)
When auditing the proposed acquisition of a new computer system, an IS auditor should FIRST establish that:

A. a clear business case has been approved by managemen
B. corporate security standards will be me
C. users will be involved in the implementation pla
D. the new system will meet all required user functionalit

Answer: A

Explanation:

The first concern of an IS auditor should be to establish that the proposal meets the needs of the business, and this should be established by a clear business case. Although compliance with security standards is essential, as is meeting the needs ofthe users and having users involved in the implementation process, it is too early in the procurement process for these to be an IS auditor's first concern.

NEW QUESTION 266
- (Topic 4)
Documentation of a business case used in an IT development project should be retained until:

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

Answer: A

Explanation:

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

NEW QUESTION 270
- (Topic 4)
To minimize the cost of a software project, quality management techniques should be applied:

A. as close to their writing (i.e., point of origination) as possibl
B. primarily at project start-up to ensure that the project is established in accordance with organizational governance standard
C. continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rat
D. mainly at project close-down to capture lessons learned that can be applied to future project

Answer: C

Explanation:

While it is important to properly establish a software development project, quality management should be effectively practiced throughout the project. The major source of unexpected costs on most software projects is rework. The general rule is thatthe earlier in the development life cycle that a defect occurs, and the longer it takes to find and fix that defect, the more effort will be needed to correct it. A well-written quality management plan is a good start, but it must also be actively applied. Simply relying on testing to identify defects is a relatively costly and less effective way of achieving software quality. For example, an error in requirements discovered in the testing phase can result in scrapping significant amounts of work. Capturing lessons learned will be too late for the current project. Additionally, applying quality management techniques throughout a project is likely to yield its own insights into the causes of quality problems and assist in staff development.

NEW QUESTION 272
- (Topic 4)
An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

A. Report that the organization does not have effective project managemen
B. Recommend the project manager be change
C. Review the IT governance structur
D. Review the conduct of the project and the business cas

Answer: D

Explanation:

Before making any recommendations, an IS auditor needs to understand the project and the factors that have contributed to making the project over budget and over schedule. The organization may have effective project management practices and sound ITgovernance and still be behind schedule or over budget. There is no indication that the project manager should be changed without looking into the reasons for the overrun.

NEW QUESTION 275
- (Topic 4)
When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

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

Answer: B

Explanation:

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

NEW QUESTION 278
- (Topic 4)
A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor
B. Database administrator
C. Project manager

D. Data owner

Answer: D

Explanation:

During the data conversion stage of a project, the data owner is primarily responsible for reviewing and signing-off that the data are migrated completely, accurately and are valid. An IS auditor is not responsible for reviewing and signing-off on the accuracy of the converted datA. However, an IS auditor should ensure that there is a review and sign-off by the data owner during the data conversion stage of the project. A database administrator's primary responsibility is to maintain the integrity of the database and make the database available to users. A database administrator is not responsible for reviewing migrated datA. A project manager provides day-to-day management and leadership of the project, but is not responsible for the accuracy and integrity of the data.

NEW QUESTION 280
- (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 281
- (Topic 4)
Information for detecting unauthorized input from a terminal would be BEST provided by the:

A. console log printou
B. transaction journa
C. automated suspense file listin
D. user error repor

Answer: B

Explanation:

The transaction journal would record all transaction activity, which then could be compared to the authorized source documents to identify any unauthorized input. A console log printout is not the best, because it would not record activity from a specific terminal. An automated suspense file listing would only list transaction activity where an edit error
occurred, while the user error report would only list input that resulted in an edit error.

NEW QUESTION 283
- (Topic 4)
Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

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

Answer: C

Explanation:

A completeness check is used to determine if a field contains data and not zeros or blanks. A check digit is a digit calculated mathematically to ensure original data were not altered. An existence check also checks entered data for agreement to predetermined criteriA. A reasonableness check matches input to predetermined reasonable limits or occurrence rates.

NEW QUESTION 285
- (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 289
- (Topic 4)
A proposed transaction processing application will have many data capture sources and outputs in paper and electronic form. To ensure that transactions are not lost during processing, an IS auditor should recommend the inclusion of:

A. validation control
B. internal credibility check
C. clerical control procedure
D. automated systems balancin

Answer: D

Explanation:

Automated systems balancing would be the best way to ensure that no transactions are lost as any imbalance between total inputs and total outputs would be reported for investigation and correction. Validation controls and internal credibility checksare certainly valid controls, but will not detect and report lost transactions. In addition, although a clerical procedure could be used to summarize and compare inputs and outputs, an automated process is less susceptible to error.

NEW QUESTION 293
- (Topic 4)
Which of the following data validation edits is effective in detecting transposition and transcription errors?

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

Answer: B

Explanation:

A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered, e.g., an incorrect, but valid, value substituted for the original. This control is effective in detecting transposition and transcription errors. A range check is checking data that matches a predetermined range of values. A validity check is programmed checking of the data validity in accordance with predetermined criteriA. In a duplicate check, newor fresh transactions are matched to those previously entered to ensure that they are not already in the system.

NEW QUESTION 295
- (Topic 4)
Which of the following is the GREATEST risk to the effectiveness of application system controls?

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

Answer: C

Explanation:

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

NEW QUESTION 299
- (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 303
- (Topic 4)
An IS auditor is told by IS management that the organization has recently reached the highest level of the software capability maturity model (CMM). The software quality process MOST recently added by the organization is:

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

Answer: A

Explanation:

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

NEW QUESTION 306
- (Topic 4)
An advantage of using sanitized live transactions in test data is that:

A. all transaction types will be include
B. every error condition is likely to be teste
C. no special routines are required to assess the result
D. test transactions are representative of live processin

Answer: D

Explanation:

Test data will be representative of live processing; however, it is unlikely that all transaction types or error conditions will be tested in this way.

NEW QUESTION 307
- (Topic 4)
Which of the following is the PRIMARY purpose for conducting parallel testing?

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

Answer: D

Explanation:

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

NEW QUESTION 310
- (Topic 4)
Which of the following should be included in a feasibility study for a project to implement an EDI process?

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

Answer: C

Explanation:

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

NEW QUESTION 315
- (Topic 4)
When a new system is to be implemented within a short time frame, it is MOST important to:

A. finish writing user manual
B. perform user acceptance testin
C. add last-minute enhancements to functionalitie
D. ensure that the code has been documented and reviewe

Answer: B

Explanation:

It would be most important to complete the user acceptance testing to ensure that the system to be implemented is working correctly. The completion of the user manuals is similar to the performance of code reviews. If time is tight, the last thing one would want to do is add another enhancement, as it would be necessary to freeze the code and complete the testing, then make any other changes as future enhancements. It would be appropriate to have the code documented and reviewed, but unless the acceptance testing is completed, there is no guarantee that the system will work correctly and meet user requirements.

NEW QUESTION 319
- (Topic 4)
A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing system developed in-house. in reviewing the proposed development approach, which of the following would be of GREATESTconcern?

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

Answer: B

Explanation:

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

NEW QUESTION 322
- (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 326
- (Topic 4)
The GREATEST benefit in implementing an expert system is the:

A. capturing of the knowledge and experience of individuals in an organizatio
B. sharing of knowledge in a central repositor
C. enhancement of personnel productivity and performanc
D. reduction of employee turnover in key department

Answer: A

Explanation:

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. Coding and entering the knowledge in a central repository, shareable within the enterprise, is a means of facilitating the expert system. Enhancing personnel productivity and performance is a benefit; however, it is not as important as capturing the knowledge and experience. Employee turnover is not necessarily affected by an expert system.

NEW QUESTION 327
- (Topic 4)
The waterfall life cycle model of software development is most appropriately used when:

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

Answer: A

Explanation:

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

NEW QUESTION 331
- (Topic 4)
The MAJOR advantage of a component-based development approach is the:

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

Answer: D

Explanation:

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

NEW QUESTION 335
- (Topic 4)
Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?

A. Parallel testing
B. Pilot testing
C. Interface/integration testing
D. Sociability testing

Answer: D

Explanation:

The purpose of sociability testing is to confirm that a new or modified system can operate in its target environment without adversely impacting existing systems. This should cover the platform that will perform primary application processing and interfaces with other systems, as well as changes to the desktop in a client-server or web development. Parallel testing is the process of feeding data into two systems-the modified system and an alternate system-and comparing the results. In this approach, the old and new systems operate concurrently for a period of time and perform the same processing functions. Pilot testing takes place first at one location and is then extended to other locations. The purpose is to see if the new system operates satisfactorily in one place before implementing it at other locations. Interface/integration testing is a hardware or software test that evaluates the connection of two or more components that pass information from one area to another.The objective is to take unit-tested modules and build an integrated structure.

NEW QUESTION 338
- (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 341
- (Topic 4)
Which of the following is an implementation risk within the process of decision support systems?

A. Management control
B. Semistructured dimensions
C. inability to specify purpose and usage patterns
D. Changes in decision processes

Answer: C

Explanation:

The inability to specify purpose and usage patterns is a risk that developers need to anticipate while implementing a decision support system (DSS). Choices A, B and D are not risks, but characteristics of a DSS.

NEW QUESTION 343
- (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 347
- (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 349
- (Topic 4)
An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

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

Answer: D

Explanation:

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

NEW QUESTION 354
- (Topic 4)
A company has implemented a new client-server enterprise resource planning (ERP) system. Local branches transmit customer orders to a central manufacturing facility. Which of the following would BEST ensure that the orders are entered accurately and the corresponding products are produced?

A. Verifying production to customer orders
B. Logging all customer orders in the ERP system
C. Using hash totals in the order transmitting process
D. Approving (production supervisor) orders prior to production

Answer: A

Explanation:

Verification will ensure that production orders match customer orders. Logging can be used to detect inaccuracies, but does not in itself guarantee accurate processing. Hash totals will ensure accurate order transmission, but not accurate processingcentrally. Production supervisory approval is a time consuming, manual process that does not guarantee proper control.

NEW QUESTION 358
- (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 361

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

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

Answer: B

Explanation:

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

NEW QUESTION 364
- (Topic 4)
An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are inplace. The BEST response the auditor can make is to:

A. review the integrity of system access control
B. accept management's statement that effective access controls are in plac
C. stress the importance of having a system control framework in plac
D. review the background checks of the accounts payable staf

Answer: C

Explanation:

Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

NEW QUESTION 368
- (Topic 4)
When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

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

Answer: A

Explanation:

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

NEW QUESTION 369
- (Topic 5)
Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?

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

Answer: D

Explanation:

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

NEW QUESTION 370
- (Topic 5)
To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?

A. System access log files
B. Enabled access control software parameters
C. Logs of access control violations

D. System configuration files for control options used

Answer: D

Explanation:

A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both systems access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

NEW QUESTION 374
- (Topic 5)
IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?

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

Answer: A

Explanation:

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

NEW QUESTION 379
- (Topic 5)
Which of the following BEST ensures the integrity of a server's operating system?

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

Answer: C

Explanation:

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

NEW QUESTION 381
- (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 383
- (Topic 5)
Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:

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

Answer: A

Explanation:

The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing and

recreational e-mail. Choice B could be true in some circumstances (i.e., it wouldneed to be implemented along with an awareness program, so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

NEW QUESTION 385
- (Topic 5)
Which of the following BEST limits the impact of server failures in a distributed environment?

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

Answer: B

Explanation:

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

NEW QUESTION 388
- (Topic 5)
When reviewing a hardware maintenance program, an IS auditor should assess whether:

A. the schedule of all unplanned maintenance is maintaine
B. it is in line with historical trend
C. it has been approved by the IS steering committe
D. the program is validated against vendor specification

Answer: D

Explanation:

Though maintenance requirements vary based on complexity and performance work loads, a hardware maintenance schedule should be validated against the vendor-provided specifications. For business reasons, an organization may choose a more aggressive maintenance program than the vendor's program. The maintenance program should include maintenance performance history, be it planned, unplanned, executed or exceptional. Unplanned maintenance cannot be scheduled. Hardware maintenance programs do not necessarily need to be in line with historical trends. Maintenance schedules normally are not approved by the steering committee.

NEW QUESTION 392
- (Topic 5)
Doing which of the following during peak production hours could result in unexpected downtime?

A. Performing data migration or tape backup
B. Performing preventive maintenance on electrical systems
C. Promoting applications from development to the staging environment
D. Replacing a failed power supply in the core router of the data center

Answer: B

Explanation:

Choices A and C are processing events which may impact performance, but would not cause downtime. Enterprise-class routers have redundant hot-swappable power supplies, so replacing a failed power supply should not be an issue. Preventive maintenanceactivities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.

NEW QUESTION 393
- (Topic 5)
Which of the following will prevent dangling tuples in a database?

A. Cyclic integrity
B. Domain integrity
C. Relational integrity
D. Referential integrity

Answer: D

Explanation:

Referential integrity ensures that a foreign key in one table will equal null or the value of a primary in the other table. For every tuple in a table having a referenced/foreign key, there should be a corresponding tuple in another table, i.e., forexistence of all foreign keys in the original tables, if this condition is not satisfied, then it results in a dangling tuple. Cyclical checking is the control technique for the regular checking of accumulated data on a file against authorized sourcedocumentation. There is no cyclical integrity testing. Domain integrity testing ensures that a data item has a legitimate value in the correct range or set. Relational integrity is performed at the record level and is ensured by calculating and verifying specific fields.

NEW QUESTION 395
- (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 396
- (Topic 5)
During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:

A. the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processe
B. there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transaction
C. the database will immediately stop execution and lose more informatio
D. the database will no longer accept input dat

Answer: A

Explanation:

When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction datA. This will normally cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be unacceptable. Choice B is incorrect, since a system can recover the corrupted external key by reindexing the table. Choices C and D would not result from a corrupted foreignkey.

NEW QUESTION 399
- (Topic 5)
A database administrator has detected a performance problem with some tables which could be solved through denormalization. This situation will increase the risk of:

A. concurrent acces
B. deadlock
C. unauthorized access to dat
D. a loss of data integrit

Answer: D

Explanation:

Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity. Deadlocks are not caused by denormalization. Access to data is controlled by defining user rights to information, and is not affected by denormalization.

NEW QUESTION 400
- (Topic 5)
An IS auditor finds that, at certain times of the day, the data warehouse query performance decreases significantly. Which of the following controls would it be relevant for the IS auditor to review?

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

Answer: C

Explanation:

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

NEW QUESTION 404
- (Topic 5)
Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server troubleshooting

Answer: A

Explanation:

Configuration management is widely accepted as one of the key components of any network, since it establishes how the network will function internally and externally, it also deals with the management of configuration and monitoring performance. Topological mappings provide outlines of the components of the network and its connectivity. Application monitoring is not essential and proxy server troubleshooting is used for troubleshooting purposes.

NEW QUESTION 407
- (Topic 5)
Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

A. Assess the impact of patches prior to installatio
B. Ask the vendors for a new software version with all fixes include
C. install the security patch immediatel
D. Decline to deal with these vendors in the futur

Answer: A

Explanation:

The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. To install the patch without knowing what it might affect could easily cause problems. New software versions withall fixes included are not always available and a full installation could be time consuming. Declining to deal with vendors does not take care of the flaw.

NEW QUESTION 409
- (Topic 5)
Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?

A. Release-to-release source and object comparison reports
B. Library control software restricting changes to source code
C. Restricted access to source code and object code
D. Date and time-stamp reviews of source and object code

Answer: D

Explanation:

Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is theone being used.

NEW QUESTION 411
- (Topic 5)
Change management procedures are established by IS management to:

A. control the movement of applications from the test environment to the production environmen
B. control the interruption of business operations from lack of attention to unresolved problem
C. ensure the uninterrupted operation of the business in the event of a disaste
D. verify that system changes are properly documente

Answer: A

Explanation:

Change management procedures are established by IS management to control the movement of applications from the test environment to the production environment. Problem escalation procedures control the interruption of business operations from lack of attention to unresolved problems, and quality assurance procedures verify that system changes are authorized and tested.

NEW QUESTION 414
- (Topic 5)
Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?

A. Review software migration records and verify approval
B. identify changes that have occurred and verify approval
C. Review change control documentation and verify approval
D. Ensure that only appropriate staff can migrate changes into productio

Answer: B

Explanation:

The most effective method is to determine through code comparisons what changes have been made and then verify that they have been approved. Change control records and software migration records may not have all changes listed. Ensuring that only appropriate staff can migrate changes into production is a key control process, but in itself does not verify compliance.

NEW QUESTION 416
- (Topic 5)

An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

A. apply the patch according to the patch's release note
B. ensure that a good change management process is in plac
C. thoroughly test the patch before sending it to productio
D. approve the patch after doing a risk assessmen

Answer: B

Explanation:

An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly. The other choices are part of a good change management process but arenot an IS auditor's responsibility.

NEW QUESTION 420
- (Topic 5)
When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:

A. allow changes, which will be completed using after-the-fact follow-u
B. allow undocumented changes directly to the production librar
C. do not allow any emergency change
D. allow programmers permanent access to production program

Answer: A

Explanation:

There may be situations where emergency fixes are required to resolve system problems. This involves the use of special logon IDs that grant programmers temporary access to production programs during emergency situations. Emergency changes should becompleted using after-the-fact follow-up procedures, which ensure that normal procedures are retroactively applied; otherwise, production may be impacted. Changes made in this fashion should be held in an emergency library from where they can be moved to the production library, following the normal change management process. Programmers should not directly alter the production library nor should they be allowed permanent access to production programs.

NEW QUESTION 425
- (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 427
- (Topic 5)
After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

A. Differential reporting
B. False-positive reporting
C. False-negative reporting
D. Less-detail reporting

Answer: C

Explanation:

False-negative reporting on weaknesses means the control weaknesses in the network are not identified and therefore may not be addressed, leaving the network vulnerable to attack. False-positive reporting is one in which the controls are in place, but are evaluated as weak, which should prompt a rechecking of the controls. Less-detail reporting and differential reporting functions provided by these tools compare scan results over a period of time.

NEW QUESTION 428
- (Topic 5)
An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

A. the setup is geographically disperse
B. the network servers are clustered in a sit
C. a hot site is ready for activatio
D. diverse routing is implemented for the networ

Answer: B

Explanation:

A clustered setup in one location makes the entire network vulnerable to natural disasters or other disruptive events. Dispersed geographical locations and diverse routing provide backup if a site has been destroyed. A hot site would also be a good alternative for a single point-of-failure site.

NEW QUESTION 429
- (Topic 5)
A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

A. Most employees use laptop
B. A packet filtering firewall is use
C. The IP address space is smaller than the number of PC
D. Access to a network port is not restricte

Answer: D

Explanation:

Given physical access to a port, anyone can connect to the internal network. The other choices do not present the exposure that access to a port does. DHCP provides convenience (an advantage) to the laptop users. Sharing IP addresses and the existence of a firewall can be security measures.

NEW QUESTION 433
- (Topic 5)
In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

A. Diskless workstations
B. Data encryption techniques
C. Network monitoring devices
D. Authentication systems

Answer: C

Explanation:

Network monitoring devices may be used to inspect activities from known or unknown users and can identify client addresses, which may assist in finding evidence of unauthorized access. This serves as a detective control. Diskless workstations preventaccess control software from being bypassed. Data encryption techniques can help protect sensitive or propriety data from unauthorized access, thereby serving as a preventive control. Authentication systems may provide environmentwide, logical facilities that can differentiate among users, before providing access to systems.

NEW QUESTION 434
- (Topic 5)
Neural networks are effective in detecting fraud because they can:

A. discover new trends since they are inherently linea
B. solve problems where large and general sets of training data are not obtainabl
C. attack problems that require consideration of a large number of input variable
D. make assumptions about the shape of any curve relating variables to the outpu

Answer: C

Explanation:

Neural networks can be used to attack problems that require consideration of numerous input variables. They are capable of capturing relationships and patterns often missed by other statistical methods, but they will not discover new trends. Neural networks are inherently nonlinear and make no assumption about the shape of any curve relating variables to the output. Neural networks will not work well at solving problems for which sufficiently large and general sets of training data are not obtainable.

NEW QUESTION 436
- (Topic 5)
In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?

A. Virus attack
B. Performance degradation
C. Poor management controls
D. Vulnerability to external hackers

Answer: B

Explanation:

Hubs are internal devices that usually have no direct external connectivity, and thus are not prone to hackers. There are no known viruses that are specific to hub attacks. While this situation may be an indicator of poor management controls, choiceB is more likely when the practice of stacking hubs and creating more terminal connections is used.

NEW QUESTION 440
- (Topic 5)
An organization provides information to its supply chain partners and customers through

an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

A. A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewal
B. Firewall policies are updated on the basis of changing requirement
C. inbound traffic is blocked unless the traffic type and connections have been specifically permitte
D. The firewall is placed on top of the commercial operating system with all installation option

Answer: D

Explanation:

The greatest concern when implementing firewalls on top of commercial operating systems is the potential presence of vulnerabilities that could undermine the security posture of the firewall platform itself. In most circumstances, when commercial firewalls are breached that breach is facilitated by vulnerabilities in the underlying operating system. Keeping all installation options available on the system further increases the risks of vulnerabilities and exploits. Using SSL for firewall administration (choice A) is important, because changes in user and supply chain partners' roles and profiles will be dynamic. Therefore, it is appropriate to maintain the firewall policies daily (choice B), and prudent to block all inbound traffic unless permitted (choice C).

NEW QUESTION 443
- (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 444
- (Topic 5)
Reverse proxy technology for web servers should be deployed if:

A. http servers' addresses must be hidde
B. accelerated access to all published pages is require
C. caching is needed for fault toleranc
D. bandwidth to the user is limite

Answer: A

Explanation:

Reverse proxies are primarily designed to hide physical and logical internal structures from outside access. Complete URLs or URIs can be partially or completely redirected without disclosing which internal or DMZ server is providing the requested datA. This technology might be used if a trade-off between security, performance and costs has to be achieved. Proxy servers cache some data but normally cannot cache all pages to be published because this depends on the kind of information the web servers provide. The ability to accelerate access depends on the speed of the back-end servers, i.e., those that are cached. Thus, without making further assumptions, a gain in speed cannot be assured, but visualization and hiding of internal structures can. If speed is an issue, a scale-out approach (avoiding adding additional delays by passing firewalls, involving more servers, etc.) would be a better solution. Due to the limited caching option, reverse proxies are not suitable for enhancing fault tolerance. User requests that are handled by reverse proxy servers are using exactly the same bandwidth as direct requests to the hosts providing the data.

NEW QUESTION 446
- (Topic 5)
When auditing a proxy-based firewall, an IS auditor should:

A. verify that the firewall is not dropping any forwarded packet
B. review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresse
C. verify that the filters applied to services such as HTTP are effectiv
D. test whether routing information is forwarded by the firewal

Answer: C

Explanation:

A proxy-based firewall works as an intermediary (proxy) between the service or application and the client, it makes a connection with the client and opens a different connection with the server and, based on specific filters and rules, analyzes all the traffic between the two connections. Unlike a packet-filtering gateway, a proxy-based firewall does not forward any packets. Mapping between media access control (MAC) and IP addresses is a task for protocols such as Address Resolution Protocol/Reverse Address Resolution Protocol (ARP/RARP).

NEW QUESTION 447
- (Topic 5)
The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

A. prevent omission or duplication of transaction

B. ensure smooth data transition from client machines to server
C. ensure that e-mail messages have accurate time stamp
D. support the incident investigation proces

Answer: D

Explanation:

During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult because a time line of events might not be easily established. Time-stamping a transaction has nothing to do with the update itself. Therefore, the possibility of omission or duplication of transactions does not exist. Data transfer has nothing to do with the time stamp. While the time stamp on an e-mailmay not be accurate, this is not a significant issue.

NEW QUESTION 450
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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