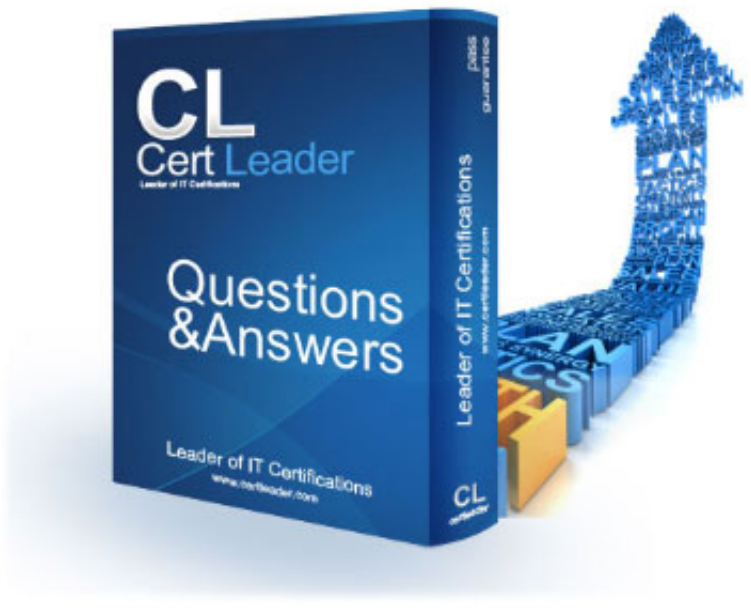
CISA Dumps

Isaca CISA

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



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

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

Answer: D

Explanation:

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

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

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

Answer: B

Explanation:

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 4
- (Topic 1)
Structured programming is BEST described as a technique that:

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

Answer: B

Explanation:

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 6
- (Topic 1)
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 7
- (Topic 1)
Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

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

Answer: C

Explanation:

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

NEW QUESTION 8
- (Topic 1)
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

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

Answer: B

Explanation:

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

NEW QUESTION 9
- (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 10

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

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

Answer: D

Explanation:

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

NEW QUESTION 10
- (Topic 1)
A 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 15
- (Topic 1)
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

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

Answer: A

Explanation:

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

NEW QUESTION 18
- (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 22
- (Topic 1)
A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

A. duplicate chec
B. table looku
C. validity chec
D. parity chec

Answer: D

Explanation:

A parity check will help to detect data errors when data are read from memory or communicated from one computer to another. A one-bit digit (either 0 or 1) is

added to a data item to indicate whether the sum of that data item's bit is odd or even. When the parity bit disagrees with the sum of the other bits, an error report is generated.

NEW QUESTION 25
- (Topic 1)
The initial step in establishing an information security program is the:

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

Answer: C

Explanation:

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

NEW QUESTION 28
- (Topic 1)
In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

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

Answer: A

Explanation:

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

NEW QUESTION 32
- (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 34
- (Topic 1)
A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

A. reasonableness chec
B. parity chec
C. redundancy chec
D. check digit

Answer: C

Explanation:

A redundancy check detects transmission errors by appending calculated bits onto the end of each segment of datA.

NEW QUESTION 39
- (Topic 1)
How does the process of systems auditing benefit from using a risk-based approach to audit planning?

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

Answer:

B

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

NEW QUESTION 40
- (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 45
- (Topic 1)
Who is ultimately accountable for the development of an IS security policy?

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

Answer: A

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

NEW QUESTION 47
- (Topic 1)
Proper segregation of duties normally does not prohibit a LAN administrator from also having programming responsibilities. True or false?

A. True
B. False

Answer: B

Explanation:
Proper segregation of duties normally prohibits a LAN administrator from also having programming responsibilities.

NEW QUESTION 51
- (Topic 1)
A core tenant of an IS strategy is that it must:

A. Be inexpensive
B. Be protected as sensitive confidential information
C. Protect information confidentiality, integrity, and availability
D. Support the business objectives of the organization

Answer: D

Explanation:
Above all else, an IS strategy must support the business objectives of the organization.

NEW QUESTION 53
- (Topic 1)
Batch control reconciliation is a _____ (fill in the blank) control for mitigating risk of inadequate segregation of duties.

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

Answer: D

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

NEW QUESTION 54
- (Topic 1)
What would an IS auditor expect to find in the console log? Choose the BEST answer.

A. Evidence of password spoofing
B. System errors
C. Evidence of data copy activities
D. Evidence of password sharing

Answer: B

Explanation:
An IS auditor can expect to find system errors to be detailed in the console log.

NEW QUESTION 55
- (Topic 1)
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 57
- (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 61
- (Topic 1)
What is an initial step in creating a proper firewall policy?

A. Assigning access to users according to the principle of least privilege
B. Determining appropriate firewall hardware and software
C. Identifying network applications such as mail, web, or FTP servers
D. Configuring firewall access rules

Answer: C

Explanation:
Identifying network applications such as mail, web, or FTP servers to be externally accessed is an initial step in creating a proper firewall policy.

NEW QUESTION 64
- (Topic 1)
What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

A. With public-key encryption, or symmetric encryption
B. With public-key encryption, or asymmetric encryption
C. With shared-key encryption, or symmetric encryption
D. With shared-key encryption, or asymmetric encryption

Answer: B

Explanation:
With public key encryption or asymmetric encryption, data is encrypted by the sender using the recipient's public key; the data is then decrypted using the recipient's private key.

NEW QUESTION 65
- (Topic 1)
Which of the following is a good control for protecting confidential data residing on a PC?

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

Answer: C

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

NEW QUESTION 69
- (Topic 1)
Which of the following is a guiding best practice for implementing logical access controls?

A. Implementing the Biba Integrity Model
B. Access is granted on a least-privilege basis, per the organization's data owners
C. Implementing the Take-Grant access control model
D. Classifying data according to the subject's requirements

Answer: B

Explanation:
Logical access controls should be reviewed to ensure that access is granted on a least-privilege basis, per the organization's data owners.

NEW QUESTION 70
- (Topic 1)
What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

A. A combination of public-key cryptography and digital certificates and two-factor authentication
B. A combination of public-key cryptography and two-factor authentication
C. A combination of public-key cryptography and digital certificates
D. A combination of digital certificates and two-factor authentication

Answer: C

Explanation:
PKI uses a combination of public-key cryptography and digital certificates to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions.

NEW QUESTION 73
- (Topic 1)
What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 77
- (Topic 1)
What is the key distinction between encryption and hashing algorithms?

A. Hashing algorithms ensure data confidentialit
B. Hashing algorithms are irreversibl
C. Encryption algorithms ensure data integrit
D. Encryption algorithms are not irreversibl

Answer: B

Explanation:
A key distinction between encryption and hashing algorithms is that hashing algorithms are irreversible.

NEW QUESTION 81
- (Topic 1)
Which of the following is used to evaluate biometric access controls?

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

Answer: B

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

NEW QUESTION 83
- (Topic 1)
Which of the following is MOST is critical during the business impact assessment phase of business continuity planning?

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

Answer: A

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

NEW QUESTION 85
- (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 89
- (Topic 1)
Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

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

Answer: A

Explanation:
Of the three major types of off-site processing facilities (hot, warm, and cold), a cold site is characterized by at least providing for electricity and HVAC. A warm site improves upon this by providing for redundant equipment and software that can be made operational within a short time.

NEW QUESTION 91
- (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 95
- (Topic 1)
Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

A. True
B. False

Answer: B

Explanation:
Function point analysis (FPA) provides an estimate of the size of an information system based on the number and complexity of a system's inputs, outputs, and files.

NEW QUESTION 97
- (Topic 1)

Who assumes ownership of a systems-development project and the resulting system?

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

Answer: A

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

NEW QUESTION 102
- (Topic 1)
When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 104
- (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 106
- (Topic 1)
Run-to-run totals can verify data through which stage(s) of application processing?

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

Answer: B

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

NEW QUESTION 110
- (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 113
- (Topic 1)
What must an IS auditor understand before performing an application audit? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 117
- (Topic 1)
Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

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

Answer: A

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

NEW QUESTION 118
- (Topic 1)
A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

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

Answer: B

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

NEW QUESTION 123
- (Topic 1)
Parity bits are a control used to validate:

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

Answer: B

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

NEW QUESTION 127
- (Topic 1)
Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

A. Proper authentication
B. Proper identification AND authentication
C. Proper identification
D. Proper identification, authentication, AND authorization

Answer: B

Explanation:
If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

NEW QUESTION 129
- (Topic 1)
To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 134

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

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

Answer: A

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

NEW QUESTION 139
- (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 140
- (Topic 1)
When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

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

Answer: A

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

NEW QUESTION 143
- (Topic 1)
The directory system of a database-management system describes:

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

Answer: B

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

NEW QUESTION 146
- (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 148
- (Topic 1)
When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

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

Answer: C

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

NEW QUESTION 152
- (Topic 1)
Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

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

Answer: C

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

NEW QUESTION 153
- (Topic 1)
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 154
- (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 156
- (Topic 1)
Which of the following can degrade network performance? Choose the BEST answer.

A. Superfluous use of redundant load-sharing gateways
B. Increasing traffic collisions due to host congestion by creating new collision domains
C. Inefficient and superfluous use of network devices such as switches
D. Inefficient and superfluous use of network devices such as hubs

Answer: D

Explanation:
Inefficient and superfluous use of network devices such as hubs can degrade network performance.

NEW QUESTION 157
- (Topic 1)
What is an effective control for granting temporary access to vendors and external support personnel? Choose the BEST answer.

A. Creating user accounts that automatically expire by a predetermined date
B. Creating permanent guest accounts for temporary use
C. Creating user accounts that restrict logon access to certain hours of the day
D. Creating a single shared vendor administrator account on the basis of least-privileged access

Answer: A

Explanation:
Creating user accounts that automatically expire by a predetermined date is an effective control for granting temporary access to vendors and external support personnel.

NEW QUESTION 158
- (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 160
- (Topic 1)
What are trojan horse programs? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 162
- (Topic 1)
Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

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

Answer: A

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

NEW QUESTION 165
- (Topic 1)
Which of the following fire-suppression methods is considered to be the most environmentally friendly?

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

Answer: C

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

NEW QUESTION 167
- (Topic 1)
Which of the following provides the BEST single-factor authentication?

A. Biometrics
B. Password
C. Token
D. PIN

Answer: A

Explanation:
Although biometrics provides only single-factor authentication, many consider it to be an excellent method for user authentication.

NEW QUESTION 170
- (Topic 1)
What should IS auditors always check when auditing password files?

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

D. That password files are archived

Answer: B

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

NEW QUESTION 175
- (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 177
- (Topic 1)
Which of the following is of greatest concern when performing an IS audit?

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

Answer: A

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

NEW QUESTION 180
- (Topic 1)
The purpose of business continuity planning and disaster-recovery planning is to:

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

Answer: B

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

NEW QUESTION 183
- (Topic 1)
An off-site processing facility should be easily identifiable externally because easy identification helps ensure smoother recovery. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 185
- (Topic 1)
How can minimizing single points of failure or vulnerabilities of a common disaster best be controlled?

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

Answer: B

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

NEW QUESTION 186
- (Topic 1)
What protects an application purchaser's ability to fix or change an application in case the application vendor goes out of business?

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

Answer: C

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

NEW QUESTION 187
- (Topic 1)
Which of the following processes are performed during the design phase of the systemsdevelopment life cycle (SDLC) model?

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

Answer: B

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

NEW QUESTION 190
- (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 191
- (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 195
- (Topic 1)
What kind of testing should programmers perform following any changes to an application or system?

A. Unit, module, and full regression testing
B. Module testing
C. Unit testing
D. Regression testing

Answer: A

Explanation:
Programmers should perform unit, module, and full regression testing
following any changes to an application or system.

NEW QUESTION 199
- (Topic 1)
Which of the following uses a prototype that can be updated continually to meet changing user or business requirements?

A. PERT
B. Rapid application development (RAD)
C. Function point analysis (FPA)
D. GANTT

Answer: B

Explanation:
Rapid application development (RAD) uses a prototype that can be updated continually to meet changing user or business requirements.

NEW QUESTION 201
- (Topic 1)
Above almost all other concerns, what often results in the greatest negative impact on the implementation of new application software?

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

Answer: A

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

NEW QUESTION 203
- (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 205
- (Topic 1)
When should an application-level edit check to verify that availability of funds was completed at the electronic funds transfer (EFT) interface?

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

Answer: D

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

NEW QUESTION 206
- (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 209
- (Topic 2)
The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

A. information assets are overprotecte
B. a basic level of protection is applied regardless of asset valu
C. appropriate levels of protection are applied to information asset
D. an equal proportion of resources are devoted to protecting all information asset

Answer: C

Explanation:

Full risk assessment determines the level of protection most appropriate to a given level of risk, while the baseline approach merely applies a standard set of protection regardless of risk. There is a cost advantage in not overprotecting information. However, an even bigger advantage is making sure that no information assets are over- or underprotected. The risk assessment approach will ensure an appropriate level of protection is applied, commensurate with the level of risk and asset value and, therefore, considering asset value. The baseline approach does not allow more resources to be directed toward the assets at greater risk, rather than equally directing resources to all assets.

NEW QUESTION 213
- (Topic 2)
Which of the following sampling methods is MOST useful when testing for compliance?

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

Answer: A

Explanation:

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

NEW QUESTION 218
- (Topic 2)
An IS auditor is assigned to perform a postimplementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

A. implemented a specific control during the development of the application syste
B. designed an embedded audit module exclusively for auditing the application syste
C. participated as a member of the application system project team, but did not have operational responsibilitie
D. provided consulting advice concerning application system best practice

Answer: A

Explanation:

Independence may be impaired if an IS auditor is, or has been, actively involved in the development, acquisition and implementation of the application system. Choices B and C are situations that do not impair an IS auditor's independence. Choice D isincorrect because an IS auditor's independence is not impaired by providing advice on known best practices.

NEW QUESTION 219
- (Topic 2)
An organization's IS audit charter should specify the:

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

Answer: D

Explanation:

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

NEW QUESTION 223
- (Topic 2)
The extent to which data will be collected during an IS audit should be determined based on the:

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

Answer: D

Explanation:

The extent to which data will be collected during an IS audit should be related directly to the scope and purpose of the audit. An audit with a narrow purpose and scope would result most likely in less data collection, than an audit with a wider purpose and scope. The scope of an IS audit should not be constrained by the

ease of obtaining the information or by the auditor's familiarity with the area being audited. Collecting all the required evidence is a required element of an IS audit, and thescope of the audit should not be limited by the auditee's ability to find relevant evidence.

NEW QUESTION 226
- (Topic 2)
While planning an audit, an assessment of risk should be made to provide:

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

Answer: A

Explanation:

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

NEW QUESTION 230
- (Topic 2)
An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

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

Answer: D

Explanation:

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

NEW QUESTION 231
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 234
- (Topic 2)
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

Answer: A

Explanation:

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

NEW QUESTION 237
- (Topic 2)
Which of the following would be the BEST population to take a sample from when testing program changes?

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

Answer: D

Explanation:

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

NEW QUESTION 239
- (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 241
- (Topic 2)
Data flow diagrams are used by IS auditors to:

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

Answer: C

Explanation:

Data flow diagrams are used as aids to graph or chart data flow and storage. They trace the data from its origination to destination, highlighting the paths and storage of datA. They do not order data in any hierarchy. The flow of the data will not necessarily match any hierarchy or data generation order.

NEW QUESTION 244
- (Topic 2)
An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

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

Answer: C

Explanation:

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

NEW QUESTION 246
- (Topic 2)
Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

A. Embedded audit module
B. Integrated test facility
C. Snapshots
D. Audit hooks

Answer: D

Explanation:

The audit hook technique involves embedding code in application systems for the examination of selected transactions. This helps an IS auditor to act before an error or an irregularity gets out of hand. An embedded audit module involves embedding specially-written software in the organization's host application system so that application systems are monitored on a selective basis. An integrated test facility is used when it is not practical to use test data, and snapshots are used when an audittrail is required.

NEW QUESTION 250
- (Topic 2)
When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

A. topology diagram
B. bandwidth usag
C. traffic analysis report
D. bottleneck location

Answer: A

Explanation:

The first step in assessing network monitoring controls should be the review of the adequacy of network documentation, specifically topology diagrams. If this information is not up to date, then monitoring processes and the ability to diagnose problems will not be effective.

NEW QUESTION 255
- (Topic 2)
An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

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

Answer: A

Explanation:

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

NEW QUESTION 256
- (Topic 2)
The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

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

Answer: A

Explanation:

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

NEW QUESTION 259
- (Topic 2)
In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

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

Answer: A

Explanation:

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes. Choice B is incorrect, because the changes made since the acquisition of the copy are not included in the copy of the software. Choice C is incorrect, as an IS auditor will have to gain this assurance separately. Choice D is incorrect, because any changes made between the time the control copy was acquired and the source code comparison is made will not be detected.

NEW QUESTION 260
- (Topic 2)
The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

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

Answer:

B

Explanation:

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

NEW QUESTION 262
- (Topic 2)
Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

A. include the statement of management in the audit repor
B. identify whether such software is, indeed, being used by the organizatio
C. reconfirm with management the usage of the softwar
D. discuss the issue with senior management since reporting this could have a negative impact on the organizatio

Answer: B

Explanation:

When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in the report. With respect to this matter, representations obtained from management cannot be independently verified. If the organization is using software that is not licensed, the auditor, to maintain objectivity and independence, must include this in the report.

NEW QUESTION 265
- (Topic 2)
After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

A. expand activities to determine whether an investigation is warrante
B. report the matter to the audit committe
C. report the possibility of fraud to top management and ask how they would like to procee
D. consult with external legal counsel to determine the course of action to be take

Answer: A

Explanation:

An IS auditor's responsibilities for detecting fraud include evaluating fraud indicators and deciding whether any additional action is necessary or whether an investigation should be recommended. The IS auditor should notify the appropriate authorities within the organization only if it has determined that the indicators of fraud are sufficient to recommend an investigation. Normally, the IS auditor does not have authority to consult with external legal counsel.

NEW QUESTION 266
- (Topic 2)
During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

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

Answer: B

Explanation:

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

NEW QUESTION 267
- (Topic 2)
An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 272
- (Topic 2)
When preparing an audit report the IS auditor should ensure that the results are supported by:

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

Answer: D

Explanation:

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

NEW QUESTION 273
- (Topic 2)
Which of the following is the key benefit of control self-assessment (CSA)?

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

Answer: A

Explanation:

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

NEW QUESTION 275
- (Topic 3)
An IT steering committee should review information systems PRIMARILY to assess:

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

Answer: A

Explanation:

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

NEW QUESTION 276
- (Topic 3)
Establishing the level of acceptable risk is the responsibility of:

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

Answer: B

Explanation:

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

NEW QUESTION 281
- (Topic 3)
Which of the following IT governance best practices improves strategic alignment?

A. Supplier and partner risks are manage
B. A knowledge base on customers, products, markets and processes is in plac
C. A structure is provided that facilitates the creation and sharing of business informatio
D. Top management mediate between the imperatives of business and technolog

Answer: D

Explanation:

Top management mediating between the imperatives of business and technology is an IT strategic alignment best practice. Supplier and partner risks being managed is a risk management best practice. A knowledge base on customers, products, markets andprocesses being in place is an IT value delivery best practice. An infrastructure being provided to facilitate the creation and sharing of business information is an IT value delivery and risk management best practice.

NEW QUESTION 283
- (Topic 3)
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

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

Answer: C

Explanation:

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

NEW QUESTION 284
- (Topic 3)
The ultimate purpose of IT governance is to:

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

Answer: A

Explanation:

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

NEW QUESTION 285
- (Topic 3)
What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

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

Answer: B

Explanation:

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

NEW QUESTION 286
- (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 291
- (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 292
- (Topic 3)
When segregation of duties concerns exist between IT support staff and end users, what would be a suitable compensating control?

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

Answer: B

Explanation:

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

NEW QUESTION 296
- (Topic 3)
To gain an understanding of the effectiveness of an organization's planning and management of investments in IT assets, an IS auditor should review the:

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

Answer: B

Explanation:

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

NEW QUESTION 300
- (Topic 3)
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

A. Senior management is aware of critical information assets and demonstrates an adequate concern for their protectio
B. Job descriptions contain clear statements of accountability for information securit
C. In accordance with the degree of risk and business impact, there is adequate funding for security effort
D. No actual incidents have occurred that have caused a loss or a public embarrassmen

Answer: B

Explanation:

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

NEW QUESTION 301
- (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 306
- (Topic 3)
Which of the following would an IS auditor consider the MOST relevant to short-term planning for an IS department?

A. Allocating resources
B. Keeping current with technology advances
C. Conducting control self-assessment
D. Evaluating hardware needs

Answer: A

Explanation:

The IS department should specifically consider the manner in which resources are allocated in the short term. Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake. Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department.

NEW QUESTION 309
- (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 313
- (Topic 3)
In an organization, the responsibilities for IT security are clearly assigned and enforced and an IT security risk and impact analysis is consistently performed. This represents which level of ranking in the information security governance maturity model?

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

Answer: B

Explanation:

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

NEW QUESTION 317
- (Topic 3)
Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

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

Answer: C

Explanation:

Without a policy defining who has the responsibility for granting access to specific systems, there is an increased risk that one could gain (be given) system access

when they should not have authorization. By assigning authority to grant access to specific users, there is a better chance that business objectives will be properly supported.

NEW QUESTION 319
- (Topic 3)
The PRIMARY objective of an audit of IT security policies is to ensure that:

A. they are distributed and available to all staf
B. security and control policies support business and IT objective
C. there is a published organizational chart with functional description
D. duties are appropriately segregate

Answer: B

Explanation:

Business orientation should be the main theme in implementing security. Hence, an IS audit of IT security policies should primarily focus on whether the IT and related security and control policies support business and IT objectives. Reviewing whether policies are available to all is an objective, but distribution does not ensure compliance. Availability of organizational charts with functional descriptions and segregation of duties might be included in the review, but are not the primary objective of an audit of security policies.

NEW QUESTION 324
- (Topic 3)
The rate of change in technology increases the importance of:

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

Answer: B

Explanation:

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

NEW QUESTION 329
- (Topic 3)
An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

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

Answer: A

Explanation:

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

NEW QUESTION 332
- (Topic 3)
Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

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

Answer: C

Explanation:

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

NEW QUESTION 334
- (Topic 3)
A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

A. Issues of privacy
B. Wavelength can be absorbed by the human body

C. RFID tags may not be removable
D. RFID eliminates line-of-sight reading

Answer: A

Explanation:

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

NEW QUESTION 338
- (Topic 3)
The PRIMARY objective of implementing corporate governance by an organization's management is to:

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

Answer: A

Explanation:

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

NEW QUESTION 342
- (Topic 3)
A benefit of open system architecture is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 345
- (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 347
- (Topic 3)
Which of the following BEST supports the prioritization of new IT projects?

A. Internal control self-assessment (CSA)
B. Information systems audit
C. Investment portfolio analysis
D. Business risk assessment

Answer: C

Explanation:

It is most desirable to conduct an investment portfolio analysis, which will present not only a clear focus on investment strategy, but will provide the rationale for terminating nonperforming IT projects. Internal control self-assessment {CSA} may highlight noncompliance to the current policy, but may not necessarily be the best source for driving the prioritization of IT projects. Like internal CSA, IS audits may provide only part of the picture for the prioritization of IT projects.

Businessrisk analysis is part of the investment portfolio analysis but, by itself, is not the best method for prioritizing new IT projects.

NEW QUESTION 352
- (Topic 3)
After the merger of two organizations, multiple self-developed legacy applications from both companies are to be replaced by a new common platform. Which of the following would be the GREATEST risk?

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

Answer: B

Explanation:

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

NEW QUESTION 357
- (Topic 3)
Is it appropriate for an IS auditor from a company that is considering outsourcing its IS processing to request and review a copy of each vendor's business continuity plan?

A. Yes, because an IS auditor will evaluate the adequacy of the service bureau's plan and assist their company in implementing a complementary pla
B. Yes, because based on the plan, an IS auditor will evaluate the financial stability of the service bureau and its ability to fulfill the contrac
C. No, because the backup to be provided should be specified adequately in the contrac
D. No, because the service bureau's business continuity plan is proprietary informatio

Answer: A

Explanation:

The primary responsibility of an IS auditor is to assure that the company assets are being safeguarded. This is true even if the assets do not reside on the immediate premises. Reputable service bureaus will have a well-designed and tested business continuity plan.

NEW QUESTION 359
- (Topic 3)
An IS auditor reviewing an outsourcing contract of IT facilities would expect it to define the:

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

Answer: C

Explanation:

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

NEW QUESTION 362
- (Topic 3)
When an organization is outsourcing their information security function, which of the following should be kept in the organization?

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

Answer: A

Explanation:

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

NEW QUESTION 364
- (Topic 3)
An organization has outsourced its help desk activities. An IS auditor's GREATEST concern when reviewing the contract and associated service level agreement

(SLA) between the organization and vendor should be the provisions for:

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

Answer: B

Explanation:

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

NEW QUESTION 369
- (Topic 3)
A poor choice of passwords and transmission over unprotected communications lines are examples of:

A. vulnerabilitie
B. threat
C. probabilitie
D. impact

Answer: A

Explanation:

Vulnerabilities represent characteristics of information resources that may be exploited by a threat. Threats are circumstances or events with the potential to cause harm to information resources. Probabilities represent the likelihood of the occurrence of a threat, while impacts represent the outcome or result of a threat exploiting a vulnerability.

NEW QUESTION 373
- (Topic 4)
The reason for establishing a stop or freezing point on the design of a new system is to:

A. prevent further changes to a project in proces
B. indicate the point at which the design is to be complete
C. require that changes after that point be evaluated for cost-effectivenes
D. provide the project management team with more control over the project desig

Answer: C

Explanation:

Projects often have a tendency to expand, especially during the requirements definition phase. This expansion often grows to a point where the originally anticipated cost-benefits are diminished because the cost of the project has increased. When this occurs, it is recommended that the project be stopped or frozen to allow a review of all of the cost-benefits and the payback period.

NEW QUESTION 374
- (Topic 4)
Change control for business application systems being developed using prototyping could be complicated by the:

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

Answer: B

Explanation:

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

NEW QUESTION 378
- (Topic 4)
Which of the following is a characteristic of timebox management?

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

Answer: C

Explanation:

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

NEW QUESTION 382
- (Topic 4)
Before implementing controls, management should FIRST ensure that the controls:

A. satisfy a requirement in addressing a risk issu
B. do not reduce productivit
C. are based on a cost-benefit analysi
D. are detective or correctiv

Answer: A

Explanation:

When designing controls, it is necessary to consider all the above aspects. In an ideal situation, controls that address all these aspects would be the best controls. Realistically, it may not be possible to design them all and cost may be prohibitive; therefore, it is necessary to first consider the preventive controls that attack the cause of a threat.

NEW QUESTION 387
- (Topic 4)
The editing/validation of data entered at a remote site would be performed MOST effectively at the:

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

Answer: D

Explanation:

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

NEW QUESTION 390
- (Topic 4)
To reduce the possibility of losing data during processing, the FIRST point at which control totals should be implemented is:

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

Answer: A

Explanation:

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

NEW QUESTION 392
- (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 396
- (Topic 4)
What process uses test data as part of a comprehensive test of program controls in a continuous online manner?

A. Test data/deck
B. Base-case system evaluation

C. Integrated test facility (ITF)
D. Parallel simulation

Answer: B

Explanation:

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

NEW QUESTION 398
- (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 401
- (Topic 4)
Failure in which of the following testing stages would have the GREATEST impact on the implementation of new application software?

A. System testing
B. Acceptance testing
C. Integration testing
D. Unit testing

Answer: B

Explanation:

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

NEW QUESTION 406
- (Topic 4)
Which of the following is the most important element in the design of a data warehouse?

A. Quality of the metadata
B. Speed of the transactions
C. Volatility of the data
D. Vulnerability of the system

Answer: A

Explanation:

Quality of the metadata is the most important element in the design of a data warehouse. A data warehouse is a copy of transaction data specifically structured for query and analysis. Metadata aim to provide a table of contents to the information stored in the data warehouse. Companies that have built warehouses believe that metadata are the most important component of the warehouse.

NEW QUESTION 408
- (Topic 4)
Which of the following is a dynamic analysis tool for the purpose of testing software modules?

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

Answer: A

Explanation:

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

NEW QUESTION 409
- (Topic 4)
The phases and deliverables of a system development life cycle (SDLC) project should be determined:

A. during the initial planning stages of the projec
B. after early planning has been completed, but before work has begu
C. throughout the work stages, based on risks and exposure
D. only after all risks and exposures have been identified and the IS auditor has recommended appropriate control

Answer: A

Explanation:

It is extremely important that the project be planned properly and that the specific phases and deliverables be identified during the early stages of the project.

NEW QUESTION 413
- (Topic 4)
A decision support system (DSS):

A. is aimed at solving highly structured problem
B. combines the use of models with nontraditional data access and retrieval function
C. emphasizes flexibility in the decision making approach of user
D. supports only structured decision making task

Answer: C

Explanation:

DSS emphasizes flexibility in the decision making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions, and supports semistructureddecision making tasks.

NEW QUESTION 417
- (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 421
- (Topic 4)
During which of the following phases in system development would user acceptance test plans normally be prepared?

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

Answer: B

Explanation:

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

NEW QUESTION 422
- (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 423
- (Topic 4)
Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

A. existence of a set of functions and their specified propertie
B. ability of the software to be transferred from one environment to anothe
C. capability of software to maintain its level of performance under stated condition
D. relationship between the performance of the software and the amount of resources use

Answer: A

Explanation:

Functionality is the set of attributes that bears on the existence of a set of functions and their specified properties. The functions are those that satisfy stated or implied needs. Choice B refers to portability, choice C refers to reliability andchoice D refers to efficiency.

NEW QUESTION 426
- (Topic 4)
The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

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

Answer: D

Explanation:

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

NEW QUESTION 431
- (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 435
- (Topic 4)
By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

A. reliable products are guarantee
B. programmers' efficiency is improve
C. security requirements are designe
D. predictable software processes are followe

Answer: D

Explanation:

By evaluating the organization's development projects against the CMM, an IS auditor determines whether the development organization follows a stable, predictable software process. Although the likelihood of success should increase as the software processes mature toward the optimizing level, mature processes do not guarantee a reliable product. CMM does not evaluate technical processes such as programming nor does it evaluate security requirements or other application controls.

NEW QUESTION 440
- (Topic 4)
Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

A. Applications may not be subject to testing and IT general controls
B. increased development and maintenance costs
C. increased application development time
D. Decision-making may be impaired due to diminished responsiveness to requests for information

Answer: A

Explanation:

End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls,quality assurance procedures, and documentation. A risk of end-user applications is that management may rely on them as much as traditional applications. End-user computing (EUC) systems typically result in reduced application development and maintenance costs, and a reduced development cycle time. EUC systems normally increase flexibility and responsiveness to management's information requests.

NEW QUESTION 443
- (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 448
- (Topic 4)
During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

A. implement data backup and recovery procedure
B. Define standards and closely monitor for complianc
C. Ensure that only authorized personnel can update the databas
D. Establish controls to handle concurrent access problem

Answer: A

Explanation:

Implementing data backup and recovery procedure is a corrective control, because backup and recovery procedures can be used to roll back database errors. Defining or establishing standards is a preventive control, while monitoring for compliance is adetective control. Ensuring that only authorized personnel can update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

NEW QUESTION 453
- (Topic 4)
In an online transaction processing system, data integrity is maintained by ensuring that a transaction is either completed in its entirety or not at all. This principle of data integrity is known as:

A. isolatio
B. consistenc
C. atomicit
D. durabilit

Answer: C

Explanation:

The principle of atomicity requires that a transaction be completed in its entirety or not at all. If an error or interruption occurs, all changes made up to that point are backed out. Consistency ensures that all integrity conditions in the databasebe maintained with each transaction. Isolation ensures that each transaction is isolated from other transactions; hence, each transaction only accesses data that are part of a consistent database state. Durability ensures that, when a transaction has been reported back to a user as complete, the resultant changes to the database will survive subsequent hardware or software failures.

NEW QUESTION 456
- (Topic 4)
Which of the following would help to ensure the portability of an application connected to a database?

A. Verification of database import and export procedures

B. Usage of a structured query language (SQL)
C. Analysis of stored procedures/triggers
D. Synchronization of the entity-relation model with the database physical schema

Answer: B

Explanation:

The use of SQL facilitates portability. Verification of import and export procedures with other systems ensures better interfacing with other systems, analyzing stored procedures/triggers ensures proper access/performance, and reviewing the design entity-relation model will be helpful, but none of these contribute to the portability of an application connecting to a database.

NEW QUESTION 457
- (Topic 4)
A company undertakes a business process reengineering (BPR) project in support of a new and direct marketing approach to its customers. Which of the following would be an IS auditor's main concern about the new process?

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

Answer: A

Explanation:

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

NEW QUESTION 461
- (Topic 4)
Which of the following represents the GREATEST potential risk in an EDI environment?

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

Answer: A

Explanation:

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

NEW QUESTION 462
- (Topic 4)
Which of the following is the MOST critical and contributes the greatest to the quality of data in a data warehouse?

A. Accuracy of the source data
B. Credibility of the data source
C. Accuracy of the extraction process
D. Accuracy of the data transformation

Answer: A

Explanation:

Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Credibility of the data source, accurate extraction processes and accurate transformation routines are all important, but would not change inaccurate data intoquality (accurate) data.

NEW QUESTION 467
- (Topic 4)
The GREATEST advantage of using web services for the exchange of information between two systems is:

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

Answer: C

Explanation:

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

NEW QUESTION 469
- (Topic 4)
When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

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

Answer: C

Explanation:

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

NEW QUESTION 474
- (Topic 4)
An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:

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

Answer: D

Explanation:

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

NEW QUESTION 478
- (Topic 4)
An IS auditor performing an application maintenance audit would review the log of program changes for the:

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

Answer: A

Explanation:

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

NEW QUESTION 480
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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