Isaca

Exam Questions CISA

Isaca CISA

NEW QUESTION 1
- (Topic 1)
Which of the following is MOST likely to result from a business process reengineering (BPR) project?

A. An increased number of people using technology
B. Significant cost savings, through a reduction in the complexity of information technology
C. A weaker organizational structures and less accountability
D. Increased information protection (IP) risk will increase

Answer: A

Explanation:

A BPR project more often leads to an increased number of people using technology, and this would be a cause for concern. Incorrect answers:
B. As BPR is often technology oriented, and this technology is usually more complex and volatile than in the past, cost savings do not often materialize in this areA.
D. There is no reason for IP to conflict with a BPR project, unless the project is not run properly.

NEW QUESTION 2
- (Topic 1)
A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

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

Answer: A

Explanation:

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

NEW QUESTION 3
- (Topic 1)
Which of the following network configuration options contains a direct link between any two host machines?

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

Answer: D

Explanation:

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

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

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

Answer: C

Explanation:

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

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

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

Answer: B

Explanation:

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

NEW QUESTION 6
- (Topic 1)
The use of a GANTT chart can:

A. aid in scheduling project task
B. determine project checkpoint
C. ensure documentation standard
D. direct the post-implementation revie

Answer: A

Explanation:

A GANTT chart is used in project control. It may aid in the identification of needed checkpoints but its primary use is in scheduling. It will not ensure the completion of documentation nor will it provide direction for the post-implementation review.

NEW QUESTION 7
- (Topic 1)
A hub is a device that connects:

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

Answer: D

Explanation:

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

NEW QUESTION 8
- (Topic 1)
Which of the following is a telecommunication device that translates data from digital form to analog form and back to digital?

A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator

Answer: B

Explanation:

A modem is a device that translates data from digital to analog and back to digital.

NEW QUESTION 9
- (Topic 1)
Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

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

Answer: A

Explanation:

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

NEW QUESTION 10
- (Topic 1)
For which of the following applications would rapid recovery be MOST crucial?

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

Answer: A

Explanation:

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

NEW QUESTION 10
- (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 12
- (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 14
- (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 17
- (Topic 1)
A primary benefit derived from an organization employing control self-assessment (CSA) techniques is that it can:

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

Answer: C

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

NEW QUESTION 18
- (Topic 1)
Who is accountable for maintaining appropriate security measures over information assets?

A. Data and systems owners

B. Data and systems users
C. Data and systems custodians
D. Data and systems auditors

Answer: A

Explanation:
Data and systems owners are accountable for maintaining appropriate security measures over information assets.

NEW QUESTION 23
- (Topic 1)
What topology provides the greatest redundancy of routes and the greatest network fault tolerance?

A. A star network topology
B. A mesh network topology with packet forwarding enabled at each host
C. A bus network topology
D. A ring network topology

Answer: B

Explanation:
A mesh network topology provides a point-to-point link between every network host. If each host is configured to route and forward communication, this topology provides the greatest redundancy of routes and the greatest network fault tolerance.

NEW QUESTION 27
- (Topic 1)
How is the time required for transaction processing review usually affected by properly implemented Electronic Data Interface (EDI)?

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

Answer: A

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

NEW QUESTION 30
- (Topic 1)
How is risk affected if users have direct access to a database at the system level?

A. Risk of unauthorized access increases, but risk of untraceable changes to the database decrease
B. Risk of unauthorized and untraceable changes to the database increase
C. Risk of unauthorized access decreases, but risk of untraceable changes to the database increase
D. Risk of unauthorized and untraceable changes to the database decrease

Answer: B

Explanation:
If users have direct access to a database at the system level, risk of unauthorized and untraceable changes to the database increases.

NEW QUESTION 34
- (Topic 1)
What is the most common purpose of a virtual private network implementation?

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

Answer: A

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

NEW QUESTION 37
- (Topic 1)
What benefit does using capacity-monitoring software to monitor usage patterns and trends provide to management? Choose the BEST answer.

A. The software can dynamically readjust network traffic capabilities based upon current usag
B. The software produces nice reports that really impress managemen
C. It allows users to properly allocate resources and ensure continuous efficiency of operation

D. It allows management to properly allocate resources and ensure continuous efficiency of operation

Answer: D

Explanation:
Using capacity-monitoring software to monitor usage patterns and trends enables management to properly allocate resources and ensure continuous efficiency of operations.

NEW QUESTION 39
- (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 41
- (Topic 1)
Which of the following best characterizes "worms"?

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

Answer: A

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

NEW QUESTION 42
- (Topic 1)
What are used as the framework for developing logical access controls?

A. Information systems security policies
B. Organizational security policies
C. Access Control Lists (ACL)
D. Organizational charts for identifying roles and responsibilities

Answer: A

Explanation:
Information systems security policies are used as the framework for developing logical access controls.

NEW QUESTION 45
- (Topic 1)
Which of the following do digital signatures provide?

A. Authentication and integrity of data
B. Authentication and confidentiality of data
C. Confidentiality and integrity of data
D. Authentication and availability of data

Answer: A

Explanation:
The primary purpose of digital signatures is to provide authentication and integrity of datA.

NEW QUESTION 47
- (Topic 1)
Regarding digital signature implementation, which of the following answers is correct?

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

Answer: C

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

NEW QUESTION 52
- (Topic 1)
Which of the following is an effective method for controlling downloading of files via FTP? Choose the BEST answer.

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

Answer: B

Explanation:
Application-layer gateways, or proxy firewalls, are an effective method for controlling downloading of files via FTP. Because FTP is an OSI application-layer protocol, the most effective firewall needs to be capable of inspecting through the application layer.

NEW QUESTION 56
- (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 57
- (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 62
- (Topic 1)
What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

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

Answer: B

Explanation:
Of the three major types of BCP tests (paper, walk-through, and preparedness), only the preparedness test uses actual resources to simulate a system crash and validate the plan's effectiveness.

NEW QUESTION 65
- (Topic 1)
What is often the most difficult part of initial efforts in application development? Choose the BEST answer.

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

Answer: C

Explanation:

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

NEW QUESTION 69
- (Topic 1)
What is a primary high-level goal for an auditor who is reviewing a system development project?

A. To ensure that programming and processing environments are segregated
B. To ensure that proper approval for the project has been obtained
C. To ensure that business objectives are achieved
D. To ensure that projects are monitored and administrated effectively

Answer: C

Explanation:
A primary high-level goal for an auditor who is reviewing a systems-development project is to ensure that business objectives are achieved. This objective guides all other systems development objectives.

NEW QUESTION 73
- (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 75
- (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 80
- (Topic 1)
_____ risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

A. Quantitative; qualitative
B. Qualitative; quantitative
C. Residual; subjective
D. Quantitative; subjective

Answer: A

Explanation:
Quantitative risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a qualitative risk assessment is more appropriate.

NEW QUESTION 84
- (Topic 1)
A check digit is an effective edit check to:

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

Answer: B

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

NEW QUESTION 86

- (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 91
- (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 94
- (Topic 1)
What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

A. Document existing internal controls
B. Perform compliance testing on internal controls
C. Establish a controls-monitoring steering committee
D. Identify high-risk areas within the organization

Answer: D

Explanation:
When implementing continuous-monitoring systems, an IS auditor's first step is to identify highrisk areas within the organization.

NEW QUESTION 98
- (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 99
- (Topic 1)
If an IS auditor finds evidence of risk involved in not implementing proper segregation of
duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

A. To advise senior managemen
B. To reassign job functions to eliminate potential frau
C. To implement compensator control
D. Segregation of duties is an administrative control not considered by an IS audito

Answer: A

Explanation:
An IS auditor's primary responsibility is to advise senior management of the risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function.

NEW QUESTION 101
- (Topic 1)
Why does an IS auditor review an organization chart?

A. To optimize the responsibilities and authority of individuals
B. To control the responsibilities and authority of individuals
C. To better understand the responsibilities and authority of individuals
D. To identify project sponsors

Answer: C

Explanation:
The primary reason an IS auditor reviews an organization chart is to better understand the responsibilities and authority of individuals.

NEW QUESTION 103
- (Topic 1)
Ensuring that security and control policies support business and IT objectives is a primary objective of:

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

Answer: A

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

NEW QUESTION 106
- (Topic 1)
When auditing third-party service providers, an IS auditor should be concerned with which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 110
- (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 114
- (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 118
- (Topic 1)
What can be implemented to provide the highest level of protection from external attack?

A. Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
B. Configuring the firewall as a screened host behind a router
C. Configuring the firewall as the protecting bastion host
D. Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Answer: A

Explanation:
Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host provides a higher level of protection from external attack than all other answers.

NEW QUESTION 120
- (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 121
- (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 124
- (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 126
- (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 128
- (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 133
- (Topic 1)
What can be used to gather evidence of network attacks?

A. Access control lists (ACL)
B. Intrusion-detection systems (IDS)
C. Syslog reporting
D. Antivirus programs

Answer: B

Explanation:
Intrusion-detection systems (IDS) are used to gather evidence of network attacks.

NEW QUESTION 137
- (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 139
- (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 144
- (Topic 1)
What is a callback system?

A. It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fail
B. It is a remote-access system whereby the user's application automatically redials the remoteaccess server if the initial connection attempt fail
C. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration databas
D. It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of tim

Answer: C

Explanation:
A callback system is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.

NEW QUESTION 149
- (Topic 1)
What type of fire-suppression system suppresses fire via water that is released from a main
valve to be delivered via a system of dry pipes installed throughout the facilities?

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

Answer: A

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

NEW QUESTION 154

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

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

Answer: C

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

NEW QUESTION 155
- (Topic 1)
What determines the strength of a secret key within a symmetric key cryptosystem?

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

Answer: B

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

NEW QUESTION 159
- (Topic 1)
What process is used to validate a subject's identity?

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

Answer: D

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

NEW QUESTION 162
- (Topic 1)
Which of the following should an IS auditor review to determine user permissions that have been granted for a particular resource? Choose the BEST answer.

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

Answer: B

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

NEW QUESTION 164
- (Topic 1)
Using the OSI reference model, what layer(s) is/are used to encrypt data?

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

Answer: C

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

NEW QUESTION 168
- (Topic 1)
When should systems administrators first assess the impact of applications or systems patches?

A. Within five business days following installation
B. Prior to installation
C. No sooner than five business days following installation

D. Immediately following installation

Answer: B

Explanation:
Systems administrators should always assess the impact of patches before installation.

NEW QUESTION 169
- (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 173
- (Topic 1)
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transference of risk to a third party such as an insurer. True or false?

A. True
B. False

Answer: A

Explanation:
Mitigating the risk and impact of a disaster or business interruption usually takes priority over transferring risk to a third party such as an insurer.

NEW QUESTION 177
- (Topic 1)
Why is a clause for requiring source code escrow in an application vendor agreement important?

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

Answer: D

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

NEW QUESTION 181
- (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 183
- (Topic 1)
When should plans for testing for user acceptance be prepared? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 187
- (Topic 1)
Input/output controls should be implemented for which applications in an integrated systems environment?

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

Answer: C

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

NEW QUESTION 188
- (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 189
- (Topic 1)
_____ (fill in the blank) should be implemented as early as data preparation to support data integrity at the earliest point possible.

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

Answer: A

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

NEW QUESTION 193
- (Topic 1)
What is used as a control to detect loss, corruption, or duplication of data?

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

Answer: C

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

NEW QUESTION 197
- (Topic 1)
Data edits are implemented before processing and are considered which of the following? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 201
- (Topic 1)
Processing controls ensure that data is accurate and complete, and is processed only through which of the following? Choose the BEST answer.

A. Documented routines
B. Authorized routines

C. Accepted routines
D. Approved routines

Answer: B

Explanation:
Processing controls ensure that data is accurate and complete, and is processed only through authorized routines.

NEW QUESTION 205
- (Topic 1)
Database snapshots can provide an excellent audit trail for an IS auditor. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 207
- (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 211
- (Topic 2)
Which of the following is a benefit of a risk-based approach to audit planning? Audit:

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

Answer: D

Explanation:

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

NEW QUESTION 212
- (Topic 2)
An audit charter should:

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

Answer: D

Explanation:

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

NEW QUESTION 214
- (Topic 2)
Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

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

Answer: A

Explanation:

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

NEW QUESTION 217
- (Topic 2)
The PRIMARY advantage of a continuous audit approach is that it:

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

Answer: C

Explanation:

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

NEW QUESTION 222
- (Topic 2)
Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

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

Answer: A

Explanation:

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

NEW QUESTION 227
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 229
- (Topic 2)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 232
- (Topic 2)
In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 234
- (Topic 2)
Which of the following would normally be the MOST reliable evidence for an auditor?

A. A confirmation letter received from a third party verifying an account balance
B. Assurance from line management that an application is working as designed
C. Trend data obtained from World Wide Web (Internet) sources
D. Ratio analysts developed by the IS auditor from reports supplied by line management

Answer: A

Explanation:

Evidence obtained from independent third parties almost always is considered to be the most reliable. Choices B, C and D would not be considered as reliable.

NEW QUESTION 236
- (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 238
- (Topic 2)
An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

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

Answer: A

Explanation:

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

NEW QUESTION 239
- (Topic 2)
Which of the following is an advantage of an integrated test facility (ITF)?

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

Answer: B

Explanation:

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

NEW QUESTION 242
- (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 247
- (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 251
- (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 256
- (Topic 2)
When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

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

Answer: C

Explanation:

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

NEW QUESTION 260
- (Topic 2)
An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

A. conclude that the controls are inadequat
B. expand the scope to include substantive testin
C. place greater reliance on previous audit
D. suspend the audi

Answer:

B

Explanation:

If the answers provided to an IS auditor's questions are not confirmed by documented procedures or job descriptions, the IS auditor should expand the scope of testing the controls and include additional substantive tests. There is no evidence that whatever controls might exist are either inadequate or adequate. Placing greater reliance on previous audits or suspending the audit are inappropriate actions as they provide no current knowledge of the adequacy of the existing controls.

NEW QUESTION 265
- (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 270
- (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 275
- (Topic 2)
Which of the following would be the MOST effective audit technique for identifying segregation of duties violations in a new enterprise resource planning (ERP) implementation?

A. Reviewing a report of security rights in the system
B. Reviewing the complexities of authorization objects
C. Building a program to identify conflicts in authorization
D. Examining recent access rights violation cases

Answer: C

Explanation:

Since the objective is to identify violations in segregation of duties, it is necessary to define the logic that will identify conflicts in authorization. A program could be developed to identify these conflicts. A report of security rights in the enterprise resource planning (ERP) system would be voluminous and time consuming to review; therefore, this technique is not as effective as building a program. As complexities increase, it becomes more difficult to verify the effectiveness of the systems and complexity is not, in itself, a link to segregation of duties. It is good practice to review recent access rights violation cases; however, it may require a significant amount of time to truly identify which violations actually resulted froman inappropriate segregation of duties.

NEW QUESTION 278
- (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 281
- (Topic 2)
During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

A. Dumping the memory content to a file
B. Generating disk images of the compromised system
C. Rebooting the system
D. Removing the system from the network

Answer: C

Explanation:

Rebooting the system may result in a change in the system state and the loss of files and important evidence stored in memory. The other choices are appropriate actions for preserving evidence.

NEW QUESTION 284
- (Topic 2)
An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

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

Answer: C

Explanation:

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

NEW QUESTION 286
- (Topic 2)
The final decision to include a material finding in an audit report should be made by the:

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

Answer: C

Explanation:

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

NEW QUESTION 287
- (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 288
- (Topic 3)
The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

A. a lack of investment in technolog

B. a lack of a methodology for systems developmen
C. technology not aligning with the organization's objective
D. an absence of control over technology contract

Answer: C

Explanation:

A steering committee should exist to ensure that the IT strategies support the organization's goals. The absence of an information technology committee or a committee not composed of senior managers would be an indication of a lack of top-level management commitment. This condition would increase the risk that IT would not be aligned with the organization's strategy.

NEW QUESTION 291
- (Topic 3)
IT governance is PRIMARILY the responsibility of the:

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

Answer: B

Explanation:

IT governance is primarily the responsibility of the executives and shareholders {as represented by the board of directors). The chief executive officer is instrumental in implementing IT governance per the directions of the board of directors. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. The audit committee reports to the board of directors and should monitor the implementation of audit recommendations.

NEW QUESTION 296
- (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 301
- (Topic 3)
Which of the following is the MOST important element for the successful implementation of IT governance?

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

Answer: B

Explanation:

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

NEW QUESTION 304
- (Topic 3)
When implementing an IT governance framework in an organization the MOST important objective is:

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

Answer: A

Explanation:

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

strategies.

NEW QUESTION 305
- (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 309
- (Topic 3)
A long-term IS employee with a strong technical background and broad managerial experience has applied for a vacant position in the IS audit department. Determining whether to hire this individual for this position should be based on the individual'sexperience and:

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

Answer: D

Explanation:

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

NEW QUESTION 310
- (Topic 3)
Which of the following controls would an IS auditor look for in an environment where duties cannot be appropriately segregated?

A. Overlapping controls
B. Boundary controls
C. Access controls
D. Compensating controls

Answer: D

Explanation:

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness that may arise when duties cannot be appropriately segregated. Overlapping controls are two controls addressing the same control objective or exposure. Since primary controls cannot be achieved when duties cannot or are not appropriately segregated, it is difficult to install overlapping controls. Boundary controls establish the interface between the would-be user of a computer system and the computer system itself, and are individual-based, not role-based, controls. Access controls for resources are based on individuals and not on roles.

NEW QUESTION 313
- (Topic 3)
Which of the following reduces the potential impact of social engineering attacks?

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

Answer: C

Explanation:

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

NEW QUESTION 314
- (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 318
- (Topic 3)
Which of the following is normally a responsibility of the chief security officer (CSO)?

A. Periodically reviewing and evaluating the security policy
B. Executing user application and software testing and evaluation
C. Granting and revoking user access to IT resources
D. Approving access to data and applications

Answer: A

Explanation:

The role of a chief security officer (CSO) is to ensure that the corporate security policy and controls are adequate to prevent unauthorized access to the company assets, including data, programs and equipment. User application and other software testing and evaluation normally are the responsibility of the staff assigned to development and maintenance. Granting and revoking access to IT resources is usually a function of network or database administrators. Approval of access to data and applications is the duty of the data owner.

NEW QUESTION 319
- (Topic 3)
An IS auditor reviewing an organization's IT strategic plan should FIRST review:

A. the existing IT environmen
B. the business pla
C. the present IT budge
D. current technology trend

Answer: B

Explanation:

The IT strategic plan exists to support the organization's business plan. To evaluate the IT strategic plan, an IS auditor would first need to familiarize themselves with the business plan.

NEW QUESTION 322
- (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 327
- (Topic 3)
To aid management in achieving IT and business alignment, an IS auditor should recommend the use of:

A. control self-assessment
B. a business impact analysi
C. an IT balanced scorecar
D. business process reengineerin

Answer: C

Explanation:

An IT balanced scorecard (BSC) 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 ability to innovate. Control self-assessment (CSA), business impact analysis (BIA) and business process reengineering (BPR) are insufficient to align IT with organizational objectives.

NEW QUESTION 331
- (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 334
- (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 337
- (Topic 3)
The development of an IS security policy is ultimately the responsibility of the:

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

Answer: D

Explanation:

Normally, the designing of an information systems security policy is the responsibility of top management or the board of directors. The IS department is responsible for the execution of the policy, having no authority in framing the policy. The security committee also functions within the broad security policy framed by the board of directors. The security administrator is responsible for implementing, monitoring and enforcing the security rules that management has established and authorized.

NEW QUESTION 341
- (Topic 3)
Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

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

Answer: A

Explanation:

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

NEW QUESTION 344
- (Topic 3)
Which of the following should be included in an organization's IS security policy?

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

Answer: B

Explanation:

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

NEW QUESTION 345
- (Topic 3)
The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

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

Answer: D

Explanation:

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

NEW QUESTION 348
- (Topic 3)
When developing a security architecture, which of the following steps should be executed FIRST?

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

Answer: B

Explanation:

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

NEW QUESTION 349
- (Topic 3)
Which of the following provides the best evidence of the adequacy of a security awareness program?

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

Answer: D

Explanation:

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

NEW QUESTION 353
- (Topic 3)
To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

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

Answer: D

Explanation:

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

tactical planning is relevant only after high-level IT investment decisions have been made.

NEW QUESTION 354
- (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 357
- (Topic 3)
Which of the following is the MOST important function to be performed by IS management when a service has been outsourced?

A. Ensuring that invoices are paid to the provider
B. Participating in systems design with the provider
C. Renegotiating the provider's fees
D. Monitoring the outsourcing provider's performance

Answer: D

Explanation:

In an outsourcing environment, the company is dependent on the performance of the service provider. Therefore, it is critical the outsourcing provider's performance be monitored to ensure that services are delivered to the company as required. Payment of invoices is a finance function, which would be completed per contractual requirements. Participating in systems design is a byproduct of monitoring the outsourcing provider's performance, while renegotiating fees is usually a one-time activity.

NEW QUESTION 360
- (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 361
- (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 364
- (Topic 3)
When performing a review of the structure of an electronic funds transfer (EFT) system, an IS auditor observes that the technological infrastructure is based on a centralized processing scheme that has been outsourced to a provider in another country. Based on this information, which of the following conclusions should be the main concern of the IS auditor?

A. There could be a question regarding the legal jurisdictio
B. Having a provider abroad will cause excessive costs in future audit
C. The auditing process will be difficult because of the distanc
D. There could be different auditing norm

Answer: A

Explanation:

In the funds transfer process, when the processing scheme is centralized in a different country, there could be legal issues of jurisdiction that might affect the right to perform a review in the other country. The other choices, though possible, are not as relevant as the issue of legal jurisdiction.

NEW QUESTION 365
- (Topic 3)
To minimize costs and improve service levels an outsourcer should seek which of the following contract clauses?

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

Answer: B

Explanation:

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

NEW QUESTION 370
- (Topic 3)
An IS auditor has been assigned to review IT structures and activities recently outsourced to various providers. Which of the following should the IS auditor determine FIRST?

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

Answer: C

Explanation:

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

NEW QUESTION 373
- (Topic 3)
With respect to the outsourcing of IT services, which of the following conditions should be of GREATEST concern to an IS auditor?

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

Answer: A

Explanation:

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

NEW QUESTION 375
- (Topic 3)
Which of the following is the MOST important IS audit consideration when an organization outsources a customer credit review system to a third-party service provider? The provider:

A. meets or exceeds industry security standard
B. agrees to be subject to external security review
C. has a good market reputation for service and experienc
D. complies with security policies of the organizatio

Answer: B

Explanation:

It is critical that an independent security review of an outsourcing vendor be obtained because customer credit information will be kept there. Compliance with security standards or organization policies is important, but there is no way to verify orprove that that is the case without an independent review. Though long experience in business and good reputation is an important factor to assess service quality, the business cannot outsource to a provider whose security control is weak.

NEW QUESTION 378
- (Topic 3)
A team conducting a risk analysis is having difficulty projecting the financial losses that could result from a risk. To evaluate the potential losses, the team should:

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

Answer: C

Explanation:

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

NEW QUESTION 380
- (Topic 3)
Assessing IT risks is BEST achieved by:

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

Answer: A

Explanation:

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

NEW QUESTION 384
- (Topic 3)
To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk:

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

Answer: C

Explanation:

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

NEW QUESTION 385
- (Topic 3)
Which of the following should be considered FIRST when implementing a risk management program?

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

Answer: A

Explanation:

Implementing risk management, as one of the outcomes of effective information security governance, would require a collective understanding of the organization's

threat, vulnerability and risk profile as a first step. Based on this, an understanding of risk exposure and potential consequences of compromise could be determined. Risk management priorities based on potential consequences could then be developed. This would provide a basis for the formulation of strategies for risk mitigation sufficient to keep the consequences from risk at an acceptable level.

NEW QUESTION 386
- (Topic 3)
As a driver of IT governance, transparency of IT's cost, value and risks is primarily achieved through:

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

Answer: A

Explanation:

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

NEW QUESTION 387
- (Topic 3)
Which of the following should be the MOST important consideration when deciding areas of priority for IT governance implementation?

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

Answer: C

Explanation:

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

NEW QUESTION 391
- (Topic 3)
During an audit, an IS auditor notices that the IT department of a medium-sized organization has no separate risk management function, and the organization's operational risk documentation only contains a few broadly described IT risks. What is the MOST appropriate recommendation in this situation?

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

Answer: D

Explanation:

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

NEW QUESTION 393
- (Topic 3)
Which of the following is the PRIMARY objective of an IT performance measurement process?

A. Minimize errors
B. Gather performance data
C. Establish performance baselines
D. Optimize performance

Answer: D

Explanation:

An IT performance measurement process can be used to optimize performance, measure and manage products/services, assure accountability and make budget decisions. Minimizing errors is an aspect of performance, but not the primary objective of performance management. Gathering performance data is a phase of IT measurement process and would be used to evaluate the performance against previously established performance baselines.

NEW QUESTION 394
- (Topic 4)

Documentation of a business case used in an IT development project should be retained until:

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

Answer: A

Explanation:

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

NEW QUESTION 399
- (Topic 4)
Which of the following risks could result from inadequate software baselining?

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

Answer: A

Explanation:

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

NEW QUESTION 401
- (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 405
- (Topic 4)
An IS auditor finds that a system under development has 12 linked modules and each item of data can carry up to 10 definable attribute fields. The system handles several million transactions a year. Which of these techniques could an IS auditor use to estimate the size of the development effort?

A. Program evaluation review technique (PERT)
B. Counting source lines of code (SLOC)
C. Function point analysis
D. White box testing

Answer: C

Explanation:

Function point analysis is an indirect method of measuring the size of an application by considering the number and complexity of its inputs, outputs and files. It is useful for evaluating complex applications. PERT is a project management techniquethat helps with both planning and control. SLOC gives a direct measure of program size, but does not allow for the complexity that may be caused by having multiple, linked modules and a variety of inputs and outputs. White box testing involves a detailed review of the behavior of program code, and is a quality assurance technique suited to simpler applications during the design and build stage of development.

NEW QUESTION 406
- (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 408
- (Topic 4)
When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

A. increases in quality can be achieved, even if resource allocation is decrease
B. increases in quality are only achieved if resource allocation is increase
C. decreases in delivery time can be achieved, even if resource allocation is decrease
D. decreases in delivery time can only be achieved if quality is decrease

Answer: A

Explanation:

The three primary dimensions of a project are determined by the deliverables, the allocated resources and the delivery time. The area of the project management triangle, comprised of these three dimensions, is fixed. Depending on the degree of freedom, changes in one dimension might be compensated by changing either one or both remaining dimensions. Thus, if resource allocation is decreased an increase in quality can be achieved, if a delay in the delivery time of the project will be accepted. The area of the triangle always remains constant.

NEW QUESTION 413
- (Topic 4)
A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

A. IS auditor
B. Database administrator
C. Project manager
D. Data owner

Answer: D

Explanation:

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

NEW QUESTION 415
- (Topic 4)
A project manager of a project that is scheduled to take 18 months to complete announces that the project is in a healthy financial position because, after 6 months, only one-sixth of the budget has been spent. The IS auditor should FIRST determine:

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

Answer: A

Explanation:

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

NEW QUESTION 420
- (Topic 4)
Information for detecting unauthorized input from a terminal would be BEST provided by the:

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

Answer: B

Explanation:

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

NEW QUESTION 422
- (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 426
- (Topic 4)
Functional acknowledgements are used:

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

Answer: A

Explanation:

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

NEW QUESTION 429
- (Topic 4)
Which of the following data validation edits is effective in detecting transposition and transcription errors?

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

Answer: B

Explanation:

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

NEW QUESTION 430
- (Topic 4)
Which of the following will BEST ensure the successful offshore development of business applications?

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

Answer: B

Explanation:

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

NEW QUESTION 435
- (Topic 4)
Which of the following is the GREATEST risk to the effectiveness of application system controls?

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

Answer: C

Explanation:

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

NEW QUESTION 436
- (Topic 4)
The MAIN purpose of a transaction audit trail is to:

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

Answer: B

Explanation:

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

NEW QUESTION 438
- (Topic 4)
An appropriate control for ensuring the authenticity of orders received in an EDI application is to:

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

Answer: C

Explanation:

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

NEW QUESTION 441
- (Topic 4)
A manufacturing firm wants to automate its invoice payment system. Objectives state that the system should require considerably less time for review and authorization and the system should be capable of identifying errors that require follow up. Which of the following would BEST meet these objectives?

A. Establishing an inter-networked system of client servers with suppliers for increased efficiencies
B. Outsourcing the function to a firm specializing in automated payments and accounts receivable/invoice processing
C. Establishing an EDI system of electronic business documents and transactions with key suppliers, computer to computer, in a standard format
D. Reengineering the existing processing and redesigning the existing system

Answer: C

Explanation:

EDI is the best answer. Properly implemented (e.g., agreements with trading partners transaction standards, controls over network security mechanisms in conjunction with application controls), EDI is best suited to identify and follow up on errors more quickly, given reduced opportunities for review and authorization.

NEW QUESTION 445
- (Topic 4)
During the audit of an acquired software package, an IS auditor learned that the software purchase was based on information obtained through the Internet, rather than from responses to a request for proposal (RFP). The IS auditor should FIRST:

A. test the software for compatibility with existing hardwar
B. perform a gap analysi
C. review the licensing polic
D. ensure that the procedure had been approve

Answer: D

Explanation:

In the case of a deviation from the predefined procedures, an IS auditor should first ensure that the procedure followed for acquiring the software is consistent with the business objectives and has been approved by the appropriate authorities. The other choices are not the first actions an IS auditor should take. They are steps that may or may not be taken after determining that the procedure used to acquire the software had been approved.

NEW QUESTION 447
- (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 448
- (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 451
- (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 453
CORRECT TEXT - (Topic 4)
Which of the following is an advantage of prototyping?

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

Answer: B

NEW QUESTION 457
- (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 460
- (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 464
- (Topic 4)
An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

A. users may prefer to use contrived data for testin
B. unauthorized access to sensitive data may resul
C. error handling and credibility checks may not be fully prove
D. the full functionality of the new process may not necessarily be teste

Answer: B

Explanation:

Unless the data are sanitized, there is a risk of disclosing sensitive data.

NEW QUESTION 465
- (Topic 4)
Which of the following is the PRIMARY purpose for conducting parallel testing?

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

Answer: D

Explanation:

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

NEW QUESTION 466
- (Topic 4)
The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

A. rule
B. decision tree
C. semantic net
D. dataflow diagram

Answer: B

Explanation:

Decision trees use questionnaires to lead a user through a series of choices until a conclusion is reached. Rules refer to the expression of declarative knowledge through the use of if-then relationships. Semantic nets consist of a graph in which nodes represent physical or conceptual objects and the arcs describe the relationship between the nodes. Semantic nets resemble a dataflow diagram and make use of an inheritance mechanism to prevent duplication of data.

NEW QUESTION 470
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

CISA Practice Exam Features:

* CISA Questions and Answers Updated Frequently

* CISA Practice Questions Verified by Expert Senior Certified Staff

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

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