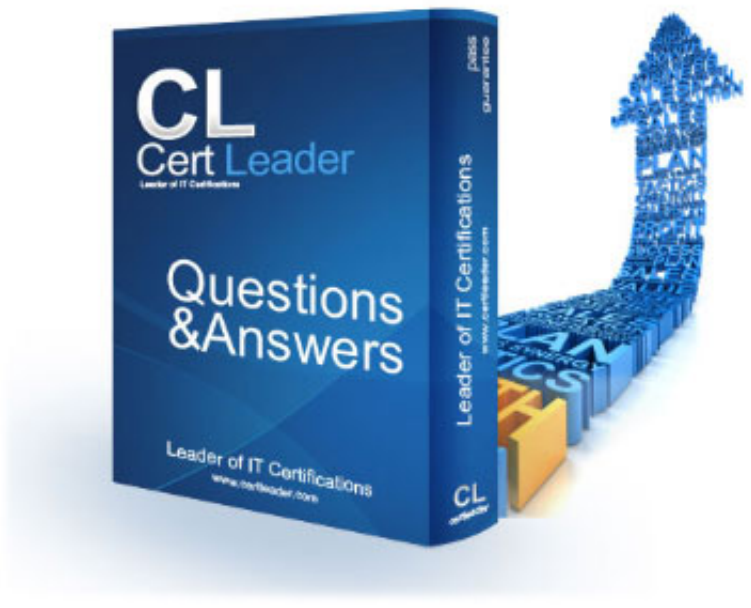
CISA Dumps

Isaca CISA

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



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

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

Answer: D

Explanation:

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 3
- (Topic 1)
Which of the following is 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 4
- (Topic 1)
Structured programming is BEST described as a technique that:

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

Answer: B

Explanation:

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

NEW QUESTION 5
- (Topic 1)
The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

A. testing stag
B. evaluation stag

C. maintenance stag
D. early stages of plannin

Answer: D

Explanation:

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

NEW QUESTION 6
- (Topic 1)
To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

A. the entire message and thereafter enciphering the message digest using the sender's private ke
B. any arbitrary part of the message and thereafter enciphering the message digest using the sender's private ke
C. the entire message and thereafter enciphering the message using the sender's private ke
D. the entire message and thereafter enciphering the message along with the message digest using the sender's private ke

Answer: A

Explanation:

A digital signature is a cryptographic method that ensures data integrity, authentication of the message, and non-repudiation. To ensure these, the sender first creates a message digest by applying a cryptographic hashing algorithm against the entire message and thereafter enciphers the message digest using the sender's private key. A message digest is created by applying a cryptographic hashing algorithm against the entire message not on any arbitrary part of the message. After creating the message digest, only the message digest is enciphered using the sender's private key, not the message.

NEW QUESTION 7
- (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 8
- (Topic 1)
Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

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

Answer: A

Explanation:

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

NEW QUESTION 9
- (Topic 1)
Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

A. Specific developments only
B. Business requirements only
C. All phases of the installation must be documented
D. No need to develop a customer specific documentation

Answer: C

Explanation:

A global enterprise product reengineering (EPR) software package can be applied to a business to replace, simplify and improve the quality of IS processing. Documentation is intended to help understand how, why and which solutions that have been selected and implemented, and therefore must be specific to the project. Documentation is also intended to support quality assurance and must be comprehensive.

NEW QUESTION 10
- (Topic 1)
Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

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

Answer: B

Explanation:

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

NEW QUESTION 10
- (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 14
- (Topic 1)
A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

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

Answer: C

Explanation:

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

NEW QUESTION 15
- (Topic 1)
What is the primary objective of a control self-assessment (CSA) program?

A. Enhancement of the audit responsibility
B. Elimination of the audit responsibility
C. Replacement of the audit responsibility
D. Integrity of the audit responsibility

Answer: A

Explanation:
Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

NEW QUESTION 16
- (Topic 1)
As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

A. The same valu
B. Greater valu
C. Lesser valu
D. Prior audit reports are not relevan

Answer: C

Explanation:
Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

NEW QUESTION 17
- (Topic 1)
After an IS auditor has identified threats and potential impacts, the auditor should:

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

Answer: A

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

NEW QUESTION 22
- (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 24
- (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 25
- (Topic 1)
What should an IS auditor do if he or she observes that project-approval procedures do not exist?

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

Answer: D

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

NEW QUESTION 26
- (Topic 1)
If senior management is not committed to strategic planning, how likely is it that a company's implementation of IT will be successful?

A. IT cannot be implemented if senior management is not committed to strategic plannin
B. More likel
C. Less likel
D. Strategic planning does not affect the success of a company's implementation of I

Answer: C

Explanation:
A company's implementation of IT will be less likely to succeed if senior management is not committed to strategic planning.

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

A. Lack of employee awareness of a company's information security policy

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

Answer: A

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

NEW QUESTION 29
- (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 31
- (Topic 1)
Atomicity enforces data integrity by ensuring that a transaction is either completed in its entirely or not at all. Atomicity is part of the ACID test reference for transaction processing. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 33
- (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 37
- (Topic 1)
What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

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

Answer: B

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

NEW QUESTION 41
- (Topic 1)
Which of the following is a good control for protecting confidential data residing on a PC?

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

Answer: C

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

NEW QUESTION 45
- (Topic 1)
What are often the primary safeguards for systems software and data?

A. Administrative access controls
B. Logical access controls
C. Physical access controls
D. Detective access controls

Answer: B

Explanation:
Logical access controls are often the primary safeguards for systems software and datA.
Which of the following is often used as a detection and deterrent control against Internet
attacks? A. Honeypots B. CCTV C. VPN D. VLAN Answer: A Honeypots are often used as a detection and deterrent control against Internet attacks.

NEW QUESTION 46
- (Topic 1)
Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

A. A monitored double-doorway entry system
B. A monitored turnstile entry system
C. A monitored doorway entry system
D. A one-way door that does not allow exit after entry

Answer: A

Explanation:
A monitored double-doorway entry system, also referred to as a mantrap or deadman door, is used as a deterrent control for the vulnerability of piggybacking.

NEW QUESTION 51
- (Topic 1)
What is the key distinction between encryption and hashing algorithms?

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

Answer: B

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

NEW QUESTION 55
- (Topic 1)
Which of the following is used to evaluate biometric access controls?

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

Answer: B

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

NEW QUESTION 59
- (Topic 1)
Who is ultimately responsible and accountable for reviewing user access to systems?

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

Answer: C

Explanation:
Data owners are ultimately responsible and accountable for reviewing user

access to systems.

NEW QUESTION 61
- (Topic 1)
Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

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

Answer: A

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

NEW QUESTION 66
- (Topic 1)
Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive
management, such as the _____. (fill-in-the-blank)

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

Answer: C

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

NEW QUESTION 70
- (Topic 1)
When is regression testing used to determine whether new application changes have
introduced any errors in the remaining unchanged code?

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

Answer: A

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

NEW QUESTION 74
- (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 76
- (Topic 1)
The quality of the metadata produced from a data warehouse is _____ in the warehouse's design. Choose the BEST answer.

A. Often hard to determine because the data is derived from a heterogeneous data environment
B. The most important consideration
C. Independent of the quality of the warehoused databases
D. Of secondary importance to data warehouse content

Answer: B

Explanation:

The quality of the metadata produced from a data warehouse is the most important consideration in the warehouse's design.

NEW QUESTION 79
- (Topic 1)
Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 84
- (Topic 1)
If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

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

Answer: B

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

NEW QUESTION 85
- (Topic 1)
Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

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

Answer: D

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

NEW QUESTION 90
- (Topic 1)
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do? Choose the BEST answer.

A. Lack of IT documentation is not usually material to the controls tested in an IT audi
B. The auditor should at least document the informal standards and policie
C. Furthermore, the IS auditor should create formal documented policies to be implemente
D. The auditor should at least document the informal standards and policies, and test for complianc
E. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemente
F. The auditor should at least document the informal standards and policies, and test for complianc
G. Furthermore, the IS auditor should create formal documented policies to be implemente

Answer: C

Explanation:
If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, the auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should recommend to management that formal documented policies be developed and implemented.

NEW QUESTION 95
- (Topic 1)
Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data-calculation procedures. True or false?

A. True
B. False

Answer: A

Explanation:

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

NEW QUESTION 99
- (Topic 1)
Run-to-run totals can verify data through which stage(s) of application processing?

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

Answer: B

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

NEW QUESTION 101
- (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 105
- (Topic 1)
What must an IS auditor understand before performing an application audit? Choose the BEST answer.

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

Answer: C

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

NEW QUESTION 106
- (Topic 1)
What is the first step in a business process re-engineering project?

A. Identifying current business processes
B. Forming a BPR steering committee
C. Defining the scope of areas to be reviewed
D. Reviewing the organizational strategic plan

Answer: C

Explanation:
Defining the scope of areas to be reviewed is the first step in a business process re-engineering project.

NEW QUESTION 110
- (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 112

- (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 117
- (Topic 1)
An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated datA. True or false?

A. True
B. False

Answer: B

Explanation:
An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated datA.

NEW QUESTION 122
- (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 123
- (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 124
- (Topic 1)
When performing an IS strategy audit, an IS auditor should review both short-term (one-year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

A. True
B. False

Answer: B

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

NEW QUESTION 129
- (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 133
- (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 138
- (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 140
- (Topic 1)
How is the risk of improper file access affected upon implementing a database system?

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

Answer: D

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

NEW QUESTION 141
- (Topic 1)
Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 145
- (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 149
- (Topic 1)
Which of the following can degrade network performance? Choose the BEST answer.

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

Answer: D

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

NEW QUESTION 150
- (Topic 1)
Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack? Choose the BEST answer.

A. Inbound traffic filtering
B. Using access control lists (ACLs) to restrict inbound connection attempts
C. Outbound traffic filtering
D. Recentralizing distributed systems

Answer: C

Explanation:
Outbound traffic filtering can help prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack.

NEW QUESTION 155
- (Topic 1)
What is a common vulnerability, allowing denial-of-service attacks?

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

Answer: C

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

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

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

Answer: D

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

NEW QUESTION 162
- (Topic 1)
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 164
- (Topic 1)
Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key. True or false?

A. False
B. True

Answer: B

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

NEW QUESTION 168
- (Topic 1)
Which of the following provides the BEST single-factor authentication?

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

Answer: A

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

NEW QUESTION 173
- (Topic 1)
What is often assured through table link verification and reference checks?

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

Answer: A

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

NEW QUESTION 177
- (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 179
- (Topic 1)
What are intrusion-detection systems (IDS) primarily used for?

A. To identify AND prevent intrusion attempts to a network
B. To prevent intrusion attempts to a network
C. Forensic incident response
D. To identify intrusion attempts to a network

Answer: D

Explanation:
Intrusion-detection systems (IDS) are used to identify intrusion attempts on a network.

NEW QUESTION 181
- (Topic 1)
If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions. True or false?

A. True
B. False

Answer: A

Explanation:
If a programmer has update access to a live system, IS auditors are more concerned with the programmer's ability to initiate or modify transactions and the ability to access production than with the programmer's ability to authorize transactions.

NEW QUESTION 184
- (Topic 1)
What is an acceptable recovery mechanism for extremely time-sensitive transaction processing?

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

Answer: C

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

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

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

Answer: B

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

NEW QUESTION 191
- (Topic 1)
What is used to develop strategically important systems faster, reduce development costs, and still maintain high quality? Choose the BEST answer.

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

Answer: A

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

NEW QUESTION 196
- (Topic 1)
What kind of testing should programmers perform following any changes to an application or system?

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

Answer: A

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

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

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

Answer: B

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

NEW QUESTION 201
- (Topic 1)
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 205
- (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 209
- (Topic 1)
Which of the following exploit vulnerabilities to cause loss or damage to the organization and its assets?

A. Exposures
B. Threats
C. Hazards
D. Insufficient controls

Answer: B

Explanation:
Threats exploit vulnerabilities to cause loss or damage to the organization and its assets.

NEW QUESTION 213
- (Topic 1)
Whenever business processes have been re-engineered, the IS auditor attempts to identify and quantify the impact of any controls that might have been removed, or controls that might not work as effectively after business process changes. True or false?

A. True
B. False

Answer: A

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

NEW QUESTION 216
- (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 221
- (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 223
- (Topic 2)
The decisions and actions of an IS auditor are MOST likely to affect which of the following risks?

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

Answer: B

Explanation:

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

NEW QUESTION 228
- (Topic 2)
An IS auditor is assigned to perform a postimplementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

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

Answer: A

Explanation:

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

NEW QUESTION 231
- (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 235
- (Topic 2)
The PRIMARY purpose of audit trails is to:

A. improve response time for user
B. establish accountability and responsibility for processed transaction
C. improve the operational efficiency of the syste
D. provide useful information to auditors who may wish to track transactions

Answer: B

Explanation:

Enabling audit trails helps in establishing the accountability and responsibility of processed transactions by tracing transactions through the system. The objective of enabling software to provide audit trails is not to improve system efficiency, since it often involves additional processing which may in fact reduce response time for users. Enabling audit trails involves storage and thus occupies disk space. Choice D is also a valid reason; however, it is not the primary reason.

NEW QUESTION 240
- (Topic 2)
When developing a risk-based audit strategy, an IS auditor should conduct a risk assessment to ensure that:

A. controls needed to mitigate risks are in plac
B. vulnerabilities and threats are identifie

C. audit risks are considere
D. a gap analysis is appropriat

Answer: B

Explanation:

In developing a risk-based audit strategy, it is critical that the risks and vulnerabilities be understood. This will determine the areas to be audited and the extent of coverage. Understanding whether appropriate controls required to mitigate risksare in place is a resultant effect of an audit. Audit risks are inherent aspects of auditing, are directly related to the audit process and are not relevant to the risk analysis of the environment to be audited. A gap analysis would normally be doneto compare the actual state to an expected or desirable state.

NEW QUESTION 243
- (Topic 2)
To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

A. schedule the audits and monitor the time spent on each audi
B. train the IS audit staff on current technology used in the compan
C. develop the audit plan on the basis of a detailed risk assessmen
D. monitor progress of audits and initiate cost control measure

Answer: C

Explanation:

Monitoring the time (choice A) and audit programs {choice D), as well as adequate training (choice B), will improve the IS audit staff's productivity (efficiency and performance), but that which delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

NEW QUESTION 247
- (Topic 2)
An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

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

Answer: D

Explanation:

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

NEW QUESTION 250
- (Topic 2)
The extent to which data will be collected during an IS audit should be determined based on the:

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

Answer: D

Explanation:

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

NEW QUESTION 253
- (Topic 2)
An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

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

Answer: A

Explanation:

Given an expected error rate and confidence level, statistical sampling is an objective method of sampling, which helps an IS auditor determine the sample size

and quantify the probability of error (confidence coefficient). Choice B is incorrect because sampling risk is the risk of a sample not being representative of the population. This risk exists for both judgment and statistical samples. Choice C is incorrect because statistical sampling does not require the use of generalized audit software. Choice D is incorrect because the tolerable error rate must be predetermined for both judgment and statistical sampling.

NEW QUESTION 258
- (Topic 2)
An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

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

Answer: A

Explanation:

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

NEW QUESTION 262
- (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 266
- (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 271
- (Topic 2)
When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

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

Answer: A

Explanation:

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

NEW QUESTION 276
- (Topic 2)
During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

A. test data to validate data inpu

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

Answer: C

Explanation:

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

NEW QUESTION 280
- (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 285
- (Topic 2)
An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

A. evaluate the record retention plans for off-premises storag
B. interview programmers about the procedures currently being followe
C. compare utilization records to operations schedule
D. review data file access records to test the librarian functio

Answer: B

Explanation:

Asking programmers about the procedures currently being followed is useful in determining whether access to program documentation is restricted to authorized persons. Evaluating the record retention plans for off-premises storage tests the recovery procedures, not the access control over program documentation. Testing utilization records or data files will not address access security over program documentation.

NEW QUESTION 290
- (Topic 2)
While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

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

Answer: C

Explanation:

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

NEW QUESTION 292
- (Topic 2)
In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

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

Answer: A

Explanation:

An IS auditor has an objective, independent and relatively complete assurance of program changes because the source code comparison will identify changes.

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

NEW QUESTION 296
- (Topic 2)
The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

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

Answer: B

Explanation:

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

NEW QUESTION 297
- (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 299
- (Topic 2)
An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

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

Answer: D

Explanation:

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

NEW QUESTION 300
- (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 304
- (Topic 2)

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

A. include the finding in the final report, because the IS auditor is responsible for an accurate report of all finding
B. not include the finding in the final report, because the audit report should include only unresolved finding
C. not include the finding in the final report, because corrective action can be verified by the IS auditor during the audi
D. include the finding in the closing meeting for discussion purposes onl

Answer: A

Explanation:

Including the finding in the final report is a generally accepted audit practice. If an action is taken after the audit started and before it ended, the audit report should identify the finding and describe the corrective action taken. An audit report should reflect the situation, as it existed at the start of the audit. All corrective actions taken by the auditee should be reported in writing.

NEW QUESTION 306
- (Topic 2)
When preparing an audit report the IS auditor should ensure that the results are supported by:

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

Answer: D

Explanation:

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

NEW QUESTION 310
- (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 311
- (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 312
- (Topic 3)
Involvement of senior management is MOST important in the development of:

A. strategic plan
B. IS policie
C. IS procedure
D. standards and guideline

Answer: A

Explanation:

Strategic plans provide the basis for ensuring that the enterprise meets its goals and objectives. Involvement of senior management is critical to ensuring that the plan adequately addresses the established goals and objectives. IS policies, procedures, standards and guidelines are all structured to support the overall strategic plan.

NEW QUESTION 315
- (Topic 3)
Establishing the level of acceptable risk is the responsibility of:

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

Answer: B

Explanation:

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

NEW QUESTION 317
- (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 318
- (Topic 3)
The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

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

Answer: C

Explanation:

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

NEW QUESTION 322
- (Topic 3)
The ultimate purpose of IT governance is to:

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

Answer: A

Explanation:

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

NEW QUESTION 324
- (Topic 3)

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

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

Answer: B

Explanation:

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

NEW QUESTION 327
- (Topic 3)
From a control perspective, the key element in job descriptions is that they:

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

Answer: D

Explanation:

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

NEW QUESTION 329
- (Topic 3)
A local area network (LAN) administrator normally would be restricted from:

A. having end-user responsibilitie
B. reporting to the end-user manage
C. having programming responsibilitie
D. being responsible for LAN security administratio

Answer: C

Explanation:

A LAN administrator should not have programming responsibilities but may have end-user responsibilities. The LAN administrator may report to the director of the IPF or, in a decentralized operation, to the end-user manager. In small organizations, the LAN administrator may also be responsible for security administration over the LAN.

NEW QUESTION 332
- (Topic 3)
An IS auditor should be concerned when a telecommunication analyst:

A. monitors systems performance and tracks problems resulting from program change
B. reviews network load requirements in terms of current and future transaction volume
C. assesses the impact of the network load on terminal response times and network data transfer rate
D. recommends network balancing procedures and improvement

Answer: A

Explanation:

The responsibilities of a telecommunications analyst include reviewing network load requirements in terms of current and future transaction volumes {choice B), assessing the impact of network load or terminal response times and network data transferrates (choice C), and recommending network balancing procedures and improvements (choice D). Monitoring systems performance and tracking problems as a result of program changes {choice A) would put the analyst in a self-monitoring role.

NEW QUESTION 336
- (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 338
- (Topic 3)
Which of the following activities performed by a database administrator (DBA) should be performed by a different person?

A. Deleting database activity logs
B. Implementing database optimization tools
C. Monitoring database usage
D. Defining backup and recovery procedures

Answer: A

Explanation:

Since database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role. A DBA should perform the other activities as part of the normal operations.

NEW QUESTION 343
- (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 346
- (Topic 3)
Which of the following is the BEST performance criterion for evaluating the adequacy of an organization's security awareness training?

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

Answer: B

Explanation:

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

NEW QUESTION 349
- (Topic 3)
Which of the following is a risk of cross-training?

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

Answer: C

Explanation:

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

NEW QUESTION 352
- (Topic 3)
In reviewing the IS short-range (tactical) plan, an IS auditor should determine whether:

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

Answer: A

Explanation:

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

NEW QUESTION 354
- (Topic 3)
Which of the following would an IS auditor consider to be the MOST important when evaluating an organization's IS strategy? That it:

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

Answer: D

Explanation:

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

NEW QUESTION 355
- (Topic 3)
When reviewing an organization's strategic IT plan an IS auditor should expect to find:

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

Answer: A

Explanation:

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

NEW QUESTION 356
- (Topic 3)
The rate of change in technology increases the importance of:

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

Answer: B

Explanation:

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

NEW QUESTION 358
- (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 362
- (Topic 3)
A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

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

Answer: B

Explanation:

Besides being a good practice, laws and regulations may require that an organization keep information that has an impact on the financial statements. The prevalence of lawsuits in which e-mail communication is held in the same regard as the officialform of classic 'paper* makes the retention of corporate e-mail a necessity. All e-mail generated on an organization's hardware is the property of the organization, and an e-mail policy should address the retention of messages, considering both known and unforeseen litigation. The policy should also address the destruction of e-mails after a specified time to protect the nature and confidentiality of the messages themselves. Addressing the retention issue in the e-mail policy would facilitate recovery, rebuilding and reuse.

NEW QUESTION 363
- (Topic 3)
A top-down approach to the development of operational policies will help ensure:

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

Answer: A

Explanation:

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

NEW QUESTION 365
- (Topic 3)
An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

A. technical platforms between the two companies are interoperabl
B. parent bank is authorized to serve as a service provide
C. security features are in place to segregate subsidiary trade
D. subsidiary can join as a co-owner of this payment syste

Answer: B

Explanation:

Even between parent and subsidiary companies, contractual agreement(s) should be in place to conduct shared services. This is particularly important in highly regulated organizations such as banking. Unless granted to serve as a service provider, itmay not be legal for the bank to extend business to the subsidiary companies. Technical aspects should always be considered; however, this can be initiated after confirming that the parent bank can serve as a service provider. Security aspects are another important factor; however, this should be considered after confirming that the parent bank can serve as a service provider. The ownership of the payment system is not as important as the legal authorization to operate the system.

NEW QUESTION 367
- (Topic 3)
IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

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

Answer: A

Explanation:

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

NEW QUESTION 368
- (Topic 3)
The PRIMARY objective of implementing corporate governance by an organization's management is to:

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

Answer: A

Explanation:

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

NEW QUESTION 373
- (Topic 3)
An example of a direct benefit to be derived from a proposed IT-related business investment is:

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

Answer: D

Explanation:

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

NEW QUESTION 375
- (Topic 3)
A benefit of open system architecture is that it:

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

Answer: A

Explanation:

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

NEW QUESTION 376
- (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 377
- (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 380
- (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 381
- (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 385
- (Topic 3)
An IS auditor should expect which of the following items to be included in the request for proposal (RFP) when IS is procuring services from an independent service provider (ISP)?

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

Answer: A

Explanation:

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

NEW QUESTION 390
- (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 391
- (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 393
- (Topic 3)
The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

A. destruction polic
B. security polic
C. archive polic
D. audit polic

Answer: C

Explanation:

With a policy of well-archived e-mail records, access to or retrieval of specific e-mail records is possible without disclosing other confidential e-mail records. Security and/or audit policies would not address the efficiency of record retrieval, and destroying e-mails may be an illegal act.

NEW QUESTION 398
- (Topic 3)
An IS auditor was hired to review e-business security. The IS auditor's first task was to examine each existing e-business application looking for vulnerabilities. What would be the next task?

A. Report the risks to the CIO and CEO immediately
B. Examine e-business application in development
C. Identify threats and likelihood of occurrence
D. Check the budget available for risk management

Answer: C

Explanation:

An IS auditor must identify the assets, look for vulnerabilities, and then identify the threats and the likelihood of occurrence. Choices A, B and D should be discussed with the CIO, and a report should be delivered to the CEO. The report should include the findings along with priorities and costs.

NEW QUESTION 401
- (Topic 3)
Which of the following does a lack of adequate security controls represent?

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

Answer: D

Explanation:

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

NEW QUESTION 405
- (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 409
- (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 410
- (Topic 3)
The IT balanced scorecard is a business governance tool intended to monitor IT performance evaluation indicators other than:

A. financial result
B. customer satisfactio
C. internal process efficienc
D. innovation capacit

Answer: A

Explanation:

Financial results have traditionally been the sole overall performance metric. The IT balanced scorecard (BSC) is an IT business governance tool aimed at monitoring IT performance evaluation indicators other than financial results. The IT BSC considers other key success factors, such as customer satisfaction, innovation capacity and processing.

NEW QUESTION 415
- (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 419
- (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 420
- (Topic 4)
Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

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

Answer: B

Explanation:

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

NEW QUESTION 422
- (Topic 4)
When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

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

Answer: B

Explanation:

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

NEW QUESTION 424
- (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 429
- (Topic 4)
A manager of a project was not able to implement all audit recommendations by the target date. The IS auditor should:

A. recommend that the project be halted until the issues are resolve
B. recommend that compensating controls be implemente
C. evaluate risks associated with the unresolved issue
D. recommend that the project manager reallocate test resources to resolve the issue

Answer: C

Explanation:

It is important to evaluate what the exposure would be when audit recommendations have not been completed by the target date. Based on the evaluation, management can accordingly consider compensating controls, risk acceptance, etc. All other choicesmight be appropriate only after the risks have been assessed.

NEW QUESTION 432
- (Topic 4)
Before implementing controls, management should FIRST ensure that the controls:

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

Answer: A

Explanation:

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

NEW QUESTION 434
- (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 437
- (Topic 4)
What control detects transmission errors by appending calculated bits onto the end of each segment of data?

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

Answer: C

Explanation:

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

NEW QUESTION 441
- (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 445
- (Topic 4)
An organization has an integrated development environment (IDE) on which the program libraries reside on the server, but modification/development and testing are done from PC workstations. Which of the following would be a strength of an IDE?

A. Controls the proliferation of multiple versions of programs
B. Expands the programming resources and aids available
C. Increases program and processing integrity
D. Prevents valid changes from being overwritten by other changes

Answer: B

Explanation:

A strength of an IDE is that it expands the programming resources and aids available. The other choices are IDE weaknesses.

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 449
- (Topic 4)
When implementing an application software package, which of the following presents the GREATEST risk?

A. Uncontrolled multiple software versions
B. Source programs that are not synchronized with object code
C. incorrectly set parameters
D. Programming error

Answer: C

Explanation:

Parameters that are not set correctly would be the greatest concern when implementing an application software package. The other choices, though important, are a concern of the provider, not the organization that is implementing the software itself.

NEW QUESTION 451
- (Topic 4)
The MOST likely explanation for the use of applets in an Internet application is that:

A. it is sent over the network from the serve
B. the server does not run the program and the output is not sent over the networ
C. they improve the performance of the web server and networ
D. it is a JAVA program downloaded through the web browser and executed by the web server of the client machin

Answer: C

Explanation:

An applet is a JAVA program that is sent over the network from the web server, through a web browser and to the client machine; the code is then run on the machine. Since the server does not run the program and the output is not sent over the network, the performance on the web server and network-over which the server and client are connected-drastically improves through the use of applets. Performance improvement is more important than the reasons offered in choices A and B. Since JAVA virtual machine (JVM) is embedded in most web browsers, the applet download through the web browser runs on the client machine from the web browser, not from the web server, making choice D incorrect.

NEW QUESTION 456
- (Topic 4)
A company has contracted with an external consulting firm to implement a commercial financial system to replace its existing system developed in-house. in reviewing the proposed development approach, which of the following would be of GREATESTconcern?

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

Answer: B

Explanation:

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

NEW QUESTION 459
- (Topic 4)
Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers

Answer: B

Explanation:

Data mining is a technique used to detect trends or patterns of transactions or datA. If the historical pattern of charges against a credit card account is changed, then it is a flag that the transaction may have resulted from a fraudulent use of the card.

NEW QUESTION 461
- (Topic 4)
Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

A. Bottom up
B. Sociability testing
C. Top-down
D. System test

Answer: C

Explanation:

The top-down approach to testing ensures that interface errors are detected early and that testing of major functions is conducted early. A bottom-up approach to testing begins with atomic units, such as programs and modules, and works upward until acomplete system test has taken place. Sociability testing and system tests take place at a later stage in the development process.

NEW QUESTION 464
- (Topic 4)
During the system testing phase of an application development project the IS auditor should review the:

A. conceptual design specification
B. vendor contrac
C. error report
D. program change request

Answer: C

Explanation:

Testing is crucial in determining that user requirements have been validated. The IS auditor should be involved in this phase and review error reports for their precision in recognizing erroneous data and review the procedures for resolving errors. Aconceptual design specification is a document prepared during the requirements definition phase. A vendor contract is prepared during a software acquisition process. Program change requests would normally be reviewed as a part of the postimplementation phase.

NEW QUESTION 468
- (Topic 4)
Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

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

Answer: A

Explanation:

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

NEW QUESTION 469
- (Topic 4)
Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

A. System owners
B. System users
C. System designers
D. System builders

Answer: A

Explanation:

System owners are the information systems (project) sponsors or chief advocates. They normally are responsible for initiating and funding projects to develop, operate and maintain information systems. System users are the individuals who use or are affected by the information system. Their requirements are crucial in the testing stage of a project. System designers translate business requirements and constraints into technical solutions. System builders construct the system based on the specifications from the systems designers. In most cases, the designers and builders are one and the same.

NEW QUESTION 470
- (Topic 4)
The MAJOR advantage of a component-based development approach is the:

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

Answer: D

Explanation:

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

NEW QUESTION 474
- (Topic 4)
The specific advantage of white box testing is that it:

A. verifies a program can operate successfully with other parts of the syste
B. ensures a program's functional operating effectiveness without regard to the internal program structur
C. determines procedural accuracy or conditions of a program's specific logic path
D. examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host syste

Answer: C

Explanation:

White box testing assesses the effectiveness of software program logic. Specifically, test data are used in determining procedural accuracy or conditions of a program's logic paths. Verifying the program can operate successfully with other parts of the system is sociability testing. Testing the program's functionality without knowledge of internal structures is black box testing. Controlled testing of programs in a semi-debugged environment, either heavily controlled step-by-step or via monitoring in virtual machines, is sand box testing.

NEW QUESTION 476
- (Topic 4)
Which of the following system and data conversion strategies provides the GREATEST redundancy?

A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run

Answer: D

Explanation:

Parallel runs are the safest-though the most expensive-approach, because both the old and new systems are run, thus incurring what might appear to be double costs. Direct cutover is actually quite risky, since it does not provide for a 'shake down period' nor does it provide an easy fallback option. Both a pilot study and a phased approach are
performedincrementally, making rollback procedures difficult to execute.

NEW QUESTION 481
- (Topic 4)
During an application audit, an IS auditor finds several problems related to corrupted data in the database. Which of the following is a corrective control that the IS auditor should recommend?

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

Answer: A

Explanation:

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

update the database is a preventive control. Establishing controls to handle concurrent access problems is also a preventive control.

NEW QUESTION 484
- (Topic 4)
An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:

A. EDI trading partner agreement
B. physical controls for terminal
C. authentication techniques for sending and receiving message
D. program change control procedure

Answer: C

Explanation:

Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

NEW QUESTION 485
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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