ISACA.CISA-KR.v2025-04-02.q544

□□□□:	CISA-KR
□□□□:	Certified Information Systems Auditor (CISA Korean Version)
□□□:	ISACA
□□ □□ □□□:	544
□□:	v2025-04-02
# □□ □:	2688
# □□ □□□:	5440
https://www.krdump.com/ISACA.CISA-KR.v2025-04-02.q544.html	

NEW QUESTION: 1
IT □□□ □□□□ □□□ □□□ □□ □□□ □□□ □□ □□□ □□□.
A. IT□ □□ □□□ □□□□□□.
B. □□□ □□□ □□ □□ □□□ □□□□□.
C. IT□ □□ □□ □□□□ □□□ □□□□.
D. IT□ □□□□ □□□□□□□.
Answer: A (LEAVE A REPLY)
Aligning IT strategy with business strategy primarily helps an organization to optimize investments in IT. This is because alignment ensures that IT resources and capabilities are aligned with the business goals and priorities, and that IT delivers value to the business in terms of efficiency, effectiveness, innovation, and competitive advantage12. By aligning IT strategy with business strategy, an organization can avoid wasting money and time on IT projects or services that do not support or contribute to the business outcomes3. Alignment also helps to identify and prioritize the most critical and valuable IT initiatives that can create or optimize business value4.
Therefore, the correct answer to your question is A. optimize investments in IT.

NEW QUESTION: 2
□□ □ IS □□□□ □□□□ □□ □□□ □□□□□□ □□ □ □□ □□ □□□ □□□ □□?
A. □□□□□□ □□□ □□ □□□ □□ □□□ □ □□□□ □□□□.
B. □□□□□ □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□□.
C. □□□□□ □□□ □□□□ □□□□□□.
D. □□□□ □□ □ □□ □□□□□ □□ □□□□ □ □□□□□.
Answer: D (LEAVE A REPLY)
Access to production source and object programs is the best way to ensure that effective change management is in place in an IS environment, as it prevents unauthorized or

accidental changes to the production code that could affect the functionality, performance, or security of the system. Access to production source and object programs should be restricted to authorized personnel only, and any changes should follow a formal change management process that includes documentation, approval, testing, and review.
References
ISACA CISA Review Manual, 27th Edition, page 254
Change Management Best Practices for the Engineering and ...
Change Management - an overview | ScienceDirect Topics

NEW QUESTION: 3
□□□ □□ □□ □□□ □□□□ □□□ □ IS □□□□ □□□ □ □□ □□ □□ □□ □ □□ □□ □ □□ □□□□?
A. □□□□ □□□□ □□
B. □□ □□□ □□
C. □□□ □□ □□
D. □□ □□□□
Answer: (SHOW ANSWER)
The best source of information for an IS auditor to use when determining whether an organization's information security policy is adequate is the risk assessment results. The risk assessment results provide the auditor with an overview of the organization's risk profile, including the identification, analysis, and evaluation of the risks that affect the confidentiality, integrity, and availability of the information assets. The auditor can use the risk assessment results to compare the organization's information security policy with the risk appetite, risk tolerance, and risk treatment strategies of the organization. The auditor can also use the risk assessment results to evaluate if the information security policy is aligned with the organization's objectives, requirements, and regulations.
Some of the web sources that support this answer are:
* Performance Measurement Guide for Information Security
* ISO 27001 Annex A.5 - Information Security Policies
* [CISA Certified Information Systems Auditor - Question0551]

NEW QUESTION: 4
□□□□ □□□ □□□□□ □□□ □□ □□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□ □□□□ □□ □□□ □□□□□ □□□.
B. □□□ □□ □□ □□□ □□ □□ □ □□ □□□ □□ □□□□□□□ □□□.
C. □□□ □□ □□ □□□ □□□ □□□□ □□□ □□ □□□□□ □□□.
D. □□□□ □□ □□ □□ □□□□□ □□□ □□□□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 5

□□ □ □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□□ □□□ □□□□ □□ □□□ □□□□□.
D. □□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Data loss can occur due to various reasons, such as accidental deletion, hardware failure, malware infection, theft, or unauthorized access. Data classification procedures can help to identify and protect sensitive data, but they are not sufficient to prevent data loss. The most effective way to protect against data loss is to conduct periodic security awareness training for employees, which can educate them on the importance of data security, the best practices for data handling and storage, and the common threats and risks to data.

NEW QUESTION: 6
IS □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□ □ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□□□□□ □□ □□□□
B. IT □□ □□
C. □□ IT □□□ □□□
D. □□ □□□□□ □□ □□
Answer: D (LEAVE A REPLY)
The most important consideration for an IS auditor when scheduling follow-up activities for agreed-upon management responses to remediate audit observations is the risk rating of original findings. The risk rating of original findings is an assessment of the potential impact or likelihood of an audit issue or observation on the organization's objectives, operations, or reputation. The risk rating of original findings can help determine the priority and urgency of follow-up activities for agreed-upon management responses to remediate audit observations by ensuring that high-risk issues are addressed first and more frequently than low-risk issues.
The other options are not as important as the risk rating of original findings in scheduling follow-up activities for agreed-upon management responses to remediate audit observations, as they do not reflect the significance or severity of audit issues or observations. Business interruption due to remediation is a possible consequence of implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. IT budgeting constraints is a possible factor that may affect the availability or feasibility of resources for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or urgency of follow-up activities. Availability of responsible IT personnel is a possible factor that may affect the accountability or responsiveness of staff for implementing corrective actions to address audit issues or observations, but it does not indicate the priority or

urgency of follow-up activities. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION: 7
□□ □ □□□ □□□ □□ □□□ □□□ □□ □□□□ □□□□□ □□ □□ □□ □□ □ □□□□□?
A. □□□ □□ □□□□ □□□ □□□ □□□□□.
B. □□, □□, □□(ETL) □□□ □□ □□□□ □□□□□.
C. □□ □□□□ □□□□□□□□ □□□ □□ □□□ □□□□□.
D. □□□ □□ □□ □□□□□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Data classification is the process of tagging data according to its type, sensitivity, and value to the organization. Data transformation is the process of changing the structure and format of data to make it usable for analysis and visualization. Both processes are important for data security and compliance, but they also pose some challenges.
One of the challenges is to ensure that the organization's data classification policies are preserved during the process of data transformation. This means that the data should retain its original classification level and labels after it is transformed, and that the appropriate controls and protections are applied to the transformed data.
The best way to ensure this is to implement classification labels in metadata during data creation (D).
Metadata is data that describes other data, such as its source, format, content, and context. By adding classification labels to metadata, the data can be easily identified and tracked throughout its lifecycle, including during data transformation. The labels can also help enforce the proper access rights and encryption standards for the data, regardless of its state or location.

NEW QUESTION: 8
□□ □ □□□□□ □□□ □□ □□ □□□ □□□□□ □□□□ □□ □□ □□□ □□ □□□?
A. □□□□ □□□ □□ □□□ □□□□□.
B. □□□□□ □□ □□□ □□ □□ □□□ □□□□□.
C. □□□□□ □□□ □□ □□□ □□□□□.
D. □□□□ □□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
□□ □ □□□ □□□ □□□ □□ □□□□ □□ □□□ □□□□□?
A. IT □□□ □□□□ □□
B. □□ □□□□ □□□
C. □□ □□□ □□□□

D. □□ □□□□ □□ □□□ □□

Answer: (SHOW ANSWER)

A computer forensic audit is a process of collecting, preserving, analyzing, and presenting digital evidence from electronic devices in a legally admissible manner. It is most relevant in situations where data loss due to hacking of servers occurs, as it can help to identify the source, method, and extent of the attack, as well as recover the lost or damaged data. The other options are not as suitable for a computer forensic audit, as they relate to internal control issues, data quality issues, or system maintenance issues, which can be addressed by other types of audits or reviews. References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.5 Computer Forensics1

NEW QUESTION: 10

□□ □ □□□□□ □□ □□□□ □□□□ □□□□ □□ □□□□□ □□□□ □□ □□ □□□?

A. □□□ □□□

B. □□□□(CA)

C. □□□□□□□

D. □□□ □□□□□

Answer: D (LEAVE A REPLY)

The most effective way to ensure the integrity of data transmitted over a network is to use a message digest. A message digest is a cryptographic function that generates a unique and fixed-length value (also known as a hash or checksum) from any input data. The message digest can be used to verify that the data has not been altered or corrupted during transmission by comparing it with the message digest generated at the destination. Message encryption is a method of protecting the confidentiality of data transmitted over a network by transforming it into an unreadable format using a secret key. Message encryption does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Certificate authority (CA) is an entity that issues and manages digital certificates that bind public keys to identities. CA does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. Steganography is a technique of hiding data within other data, such as images or audio files. Steganography does not ensure the integrity of data, as it does not prevent or detect unauthorized modifications. References:

* CISA Review Manual, 27th Edition, pages 383-3841
* CISA Review Questions, Answers & Explanations Database, Question ID: 258

NEW QUESTION: 11

□□ □ IT □□□ □□ □□□ □□□□ □□ □□ □ □□□□ □□ □□□□□?

A. IT □□ □□ □□

B. □□ □□□□□ 2□□□ □□

C. □□ □□□ □□
D. □□□ □□□□□ □□
Answer: D (LEAVE A REPLY)
Quarterly steering committee meetings best demonstrate alignment of the IT department with the corporate mission because they provide a regular forum for strategic planning, decision making, and communication between IT leaders and business stakeholders12. Steering committee meetings help to ensure that IT goals and initiatives are aligned with the business vision, mission, and objectives, and that IT performance and value are monitored and evaluated34.
References
1: IT Governance and the Balanced Scorecard - ISACA Journal
2: IT Steering Committee Best Practices: A Recipe for Success
3: What is IT Governance? - Definition from Techopedia
4: CISA Cybersecurity Strategic Plan | CISA

NEW QUESTION: 12
□□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □ □□□ □□ □ □□□(PKI)□ □□□□ □□□□□.
B. □ □□□ □□□ □□□□ □□□□□.
C. □ □□□ □□□ □□□ □□□□□□ □□□□□.
D. □ □□□ 128□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The greatest concern to an IS auditor reviewing an organization's method to transport sensitive data between offices is that the method relies exclusively on the use of asymmetric encryption algorithms. Asymmetric encryption algorithms, also known as public key encryption, use two different keys for encryption and decryption: a public key that is shared with anyone who wants to communicate with the sender, and a private key that is kept secret by the sender. Asymmetric encryption algorithms are more secure than symmetric encryption algorithms, which use the same key for both encryption and decryption, but they are also slower and more computationally intensive. Therefore, relying exclusively on asymmetric encryption algorithms may not be efficient or practical for transporting large amounts of sensitive data between offices. A better method would be to use a combination of symmetric and asymmetric encryption algorithms, such as using asymmetric encryption to exchange a symmetric key and then using symmetric encryption to encrypt and decrypt the data.
The other options are not as concerning as option C. The method relying exclusively on the use of public key infrastructure (PKI) is not a concern, because PKI is a system that provides the services and mechanisms for creating, managing, distributing, using, storing, and revoking digital certificates that are based on asymmetric encryption algorithms. PKI enables secure and authenticated communication between parties who do not have a prior

trust relationship. The method relying exclusively on the use of digital signatures is not a concern, because digital signatures are a way of verifying the authenticity and integrity of a message or document by using asymmetric encryption algorithms. Digital signatures ensure that the sender cannot deny sending the message or document, and that the receiver can detect any tampering or alteration of the message or document. The method relying exclusively on the use of 128-bit encryption is not a concern, because 128- bit encryption is a level of encryption that uses a 128-bit key to encrypt and decrypt data. 128-bit encryption is considered to be strong enough to resist brute-force attacks by modern computers. References: Asymmetric vs Symmetric Encryption: What are differences?, Public Key Infrastructure (PKI), Digital Signature, What is
128-bit Encryption?

NEW QUESTION: 13
□□□□ □□□ □□ □□□□□□□ □□□□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□□ □□□□□. □□ □ □□□□□□ □□ □□□ □□□□ □□□□□ □□ □□ □□ □□□ □□□□□?
A. □□□ □□□
B. □□□ □□
C. □□ □□□ □□□
D. □□ □□□□ □□ □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
IS □□□□ RPA(□□ □□□□ □□□) □□□ □□□ □ □□ □ □□ □□ □□□ □□ □□□?
A. □□□ □□□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□ □□□□□.
C. □□□ □□□□□ □□□□ □□□□□ □□□□□.
D. □□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 15
□□□ IT □□ □□□□ □□□ □□ □□□□ □□□ □□ □□□□ □□□□□□. □□ □□□ □□ □□□ □□□□ □□□.
A. □□ □□□ □□□□ □□□□□.
B. □□ □□ □□□ □□.
C. □□ □□□□ □□ □□ □□.
D. □□ □□□ □□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
A top-down approach in the development of IT policies means that the policies are derived from the strategic objectives and goals of the organization, and are aligned with the

business needs and expectations. This should result in greater consistency across the organization, as the policies will be coherent, integrated and applicable to all levels and functions of the organization. A bottom-up approach, on the other hand, means that the policies are developed by individual units or departments based on their operational needs and preferences, which may lead to inconsistency, duplication orconflict among different policies. References: ISACA Frameworks: Blueprints for Success, IT Governance and Process Maturity

NEW QUESTION: 16
IS □□□□ □□ □□□ □□ □□ □□□ □ □□□□□□□□ □□ □□□ □□□□□ □□□□□ □□□ □□□□□□. □□□ □□ □□□ □□□ □□□ □□□ □□□□ □□ □□□.
A. □□.
B. □□□ □□(DoS)
C. □□□□ □□ □□(SQL) □□
D. □□ □□□□
Answer: C (LEAVE A REPLY)
Moving validation controls from the server side into the browser would most likely increase the risk of a successful attack by structured query language (SQL) injection. SQL injection is a technique that exploits a security vulnerability in an application's database layer by inserting malicious SQL statements into user input fields. Validation controls are used to check and filter user input before sending it to the database. If these controls are moved to the browser, they can be easily bypassed or modified by an attacker, who can then execute arbitrary SQL commands on the database. References: CISA Review Manual, 27th Edition, page 361

NEW QUESTION: 17
□□ □□ □□□□ □ □□ □□□ □□□ □□□□.
A. □□□ □□ □□□ □□□ □□ □□□□□.
B. □□□ □□□□ □□□ □ □□ □□ □□□□ □□ □□□ □ □□□□.
C. □□□ □□ □□ □□□ □□□□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

Monetary unit sampling (MUS) is a statistical sampling method that is used to determine if the account balances or monetary amounts in a population contain any misstatements. MUS treats each individual dollar in the population as a separate sampling unit, so that larger balances or amounts have a higher probability of being selected than smaller ones. MUS then projects the results of testing the sample to the entire population in terms of dollar values, rather than error rates.
One advantage of MUS is that it increases the likelihood of selecting material items from the population.
Material items are those that have a significant impact on the financial statements and could influence the decisions of users. By giving more weight to larger items, MUS ensures that material misstatements are more likely to be detected and reported. MUS also reduces the sample size required to achieve a desired level of confidence and precision, as compared to other sampling methods that do not consider the value of items.
References:
* 4: Monetary unit sampling definition - AccountingTools
* 5: How Does Monetary Unit Sampling Work? - dummies
* 6: Audit sampling | ACCA Qualification | Students | ACCA Global

NEW QUESTION: 18
□□ □□□□ □□ □□ □□□□ □□□ □□ □□ □□ □□□ □□□□ □□□□.
IS □□□□ □□ □□□□ □□□ □ □□□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□□□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□□□ □□ □□□□ □□□□ □□□ □□□□□.
C. □□ □□□□ □□□ □□ □□□ □□□□ □□□ □□□□□□.
D. □□ □□ □□□□□ □□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
The IS auditor's best course of action when preparing the final report is to include the position supported by senior management in the final engagement report. The IS auditor should communicate the audit findings and recommendations to senior management and obtain their feedback and approval before issuing the final report. If there is a disagreement between the auditee and the IS auditor regarding a recommendation for corrective action, the IS auditor should present both sides of the argument and the supporting evidence, and seek senior management's opinion and decision. The IS auditor should respect and follow senior management' s position, and include it in the final engagement report, along with the auditee's comments if applicable. The other options arenot the best course of action, because they either do not resolve the disagreement, do notreflect senior management's authority, or do not report the audit results accurately and completely. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.5

NEW QUESTION: 19

IS □□□□ □□ □□□ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □□ □□□□. □□□□ □□ □ □□ □□ □□□ □□ □□□□ □□□□ □□□?

A. □□□ □□□ □□□□□□ □□□□.

B. □□□ □□□□ □□ □□□□ □□□□.

C. □□ □□□□□ □□□□□ □□□□□.

D. □□ □□□□□□ □□□ □□□□ □□□□.

Answer: (SHOW ANSWER)

The most critical finding that the IS auditor should consider when reviewing processes for importing market price data from external data providers is that the quality of the data is not monitored. This is because market price data is essential for financial transactions, risk management, valuation and reporting, and any errors or inaccuracies in the data can have significant impact on the organization's performance, reputation and compliance. The IS auditor should ensure that the organization has established quality criteria and controls for the imported data, such as validity, completeness, timeliness, consistency and accuracy, and that the data is regularly checked and verified against these criteria. The other findings are also important, but not as critical as data quality. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

NEW QUESTION: 20

□□□ □□ □□□ □□□(EUC)□ □□□ □, □□ □ □□ □□□ □□ □ □□□□ □□ □?

A. EUC □□ □□ □ □□□ □□□□□ □ □□

B. □□□□□ □□□ □□□□□□□.

C. IT □□□ □□ □□

D. □□ □□□□□ □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

□□ □□ □□□ □□ □□ □□□□□ □□□□□ □□□.

A. □□□□ □□□ □.

B. □□ □□ □.

C. □□ □□□ □□□□.

D. □□ □□□ □

Answer: B (LEAVE A REPLY)

Audit observations are the findings and recommendations that result from an audit engagement. Audit observations should be first communicated with the auditee during fieldwork, which is the stage of the audit process where the auditor collects and analyzes evidence to evaluate the audit objectives1. Communicating audit observations during fieldwork has several benefits, such as2:

It allows the auditor to verify the accuracy and completeness of the observations, and to obtain additional information or clarification from the auditee if needed.

It enables the auditor to discuss the root causes, impacts, and risks of the observations, and to solicit the auditee's input on possible corrective actions and implementation timelines.
It helps to build rapport and trust between the auditor and the auditee, and to avoid surprises or disagreements at the end of the audit.
It facilitates timely resolution of audit observations, and reduces the risk of audit delays or disputes.
Therefore, option B is the correct answer.
Option A is not correct because communicating audit observations when drafting the report is too late, as it may lead to misunderstandings, conflicts, or revisions that could have been avoided if the observations were communicated earlier. Option C is not correct because communicating audit observations at the end of fieldwork is also not ideal, as it may not leave enough time for the auditor and the auditee to discuss and agree on the observations and recommendations. Option D is not correct because communicating audit observations within the audit report is the final step of the audit process, not the first.
References:
Audit Process Overview1
Communicating Internal Audit Findings: Best Practices for Success2

NEW QUESTION: 22
□□ □□□□□ □□ □□□□□ □□□□ □□ □ □□ □□ □□ □□□ □□ □□□□ □ □□□ □ □□□□?
A. □ □□ □□ □□□□ □□□ □□
B. □□ □□□ □□ □□□ □□ □ □□ □□□
C. □□ □□□□□□ □□ □□□ □□
D. □□□□□ □□□ □ □□
Answer: C (LEAVE A REPLY)
Access controls for source libraries are the features of a library control software package that would protect against unauthorized updating of source code. Access controls are the mechanisms that regulate who can access, modify, or delete the source code stored in the source libraries. Source libraries are the repositories that contain the source code files and their versions. By implementing access controls for source libraries, the library control software package can prevent unauthorized or malicious users from tampering with the source code and compromising its integrity, security, or functionality1.
The other options are not as effective as access controls for source libraries in protecting against unauthorized updating of source code. Option A, required approvals at each life cycle step, is a good practice but may not be sufficient to prevent unauthorized updates if the approval process is bypassed or compromised. Option B, date and time stamping of source and object code, is a useful feature but may not prevent unauthorized updates if the date and time stamps are altered or ignored. Option D, release-to-release comparison of

source code, is a helpful feature but may not prevent unauthorized updates if the comparison results are not reviewed or acted upon.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* How to protect your source code from attackers2
* How to Stop Unauthorized Use of Open Source Code

NEW QUESTION: 23
□□ □ □□ □□ □□□ □□□ □□□ □□□ □□□□□ □□ □ □□ □□□ □□□?
A. □□ □□ □□ □□
B. □□ □□□ □□
C. □□ □□ □□□ □□
D. □□ □□ □□ □□
Answer: D (LEAVE A REPLY)
Implementing incident escalation procedures is the best way to ensure that an incident receives attention from appropriate personnel in a timely manner, because it defines the roles and responsibilities, communication channels, and escalation criteria for handlingdifferent types of incidents34. Incident escalation procedures help to prioritize and coordinate the response efforts and ensure that the incident is resolved by the most qualified and authorized personnel. Completing the incident management log, broadcasting an emergency message, and requiring a dedicated incident response team are not sufficient to ensure that an incident receives attention from appropriate personnel in a timely manner, because they do not specify how to escalate the incident based onits severity, impact,or complexity. References: 3: CISA Review Manual (Digital Version), Chapter 6, Section 6.3.2 4: CISA Online Review Course, Module 6, Lesson 3

NEW QUESTION: 24
□□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□ □□ □□(CSA)
B. □□ □□□□□ □□□
C. □□ □□
D. □□□□ □□ □□
Answer: D (LEAVE A REPLY)
Benford's law analysis is a powerful technique for identifying irregularities or anomalies in numerical datasets, such as financial transactions. It detects deviations from expected frequency distributions, which may indicate fraud.
* Control Self-Assessments (CSAs) (Option A):Useful for control evaluation but not for fraud detection.

* Interviews with Control Owners (Option B):Provide insights but are not efficient for identifying fraudulent patterns.
* Regression Analysis (Option C):Effective for predictive modeling but less so for detecting fraud in transactional data.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 25
□□ □ □□□□□□ □□□□□ □□□□□(API) □□ □□□ □□□ □□ □□□ □□□ □ □□ IS □□□□ □□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□(XML) □□□ □□□□□□.
B. API □□□□□□ □□□□□□.
C. □□ □□ □□(TLS)□ □□□□□.
D. SOAP(Simple Object Access Protocol)□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 26
□□□ □□□ □, □□□□ □□ □□□ □□□□□ □ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□ □□
C. □□□□□□
D. □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
IS □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□□ □□ □□ □□ □□□ □ □ □□□, □ □□ □□□ □□ □□ □□□□ □□□ □□□□ □□□?
A. □□□□ □□ □□□□ □□□□ □□□□.
B. □□□□ □□□ □□□ □□□□□□□□ □□ □□□□ □□□□□.
C. □□□□ □□□ □□□ □□□□□ □□□□□.
D. □□□□ □□ □□□□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
The finding that should be ranked as the highest risk is that network penetration tests are not performed.
Network penetration tests are simulated cyberattacks that aim to identify and exploit the vulnerabilities and weaknesses of the network security controls, such as firewalls, routers, switches, servers, and devices.
Network penetration tests are essential for assessing the effectiveness and resilience of the network security posture, and for providing recommendations for improvement and remediation. If network penetration tests are not performed, the organization may not be

aware of the existing or potential threats and risks to its network, and may not be able to prevent or respond to real cyberattacks, which can result in data breaches, service disruptions, financial losses, reputational damage, and legal or regulatory penalties. The other findings are also important, butnot as risky as the lack of network penetration tests, because they either do not directly affect the networksecurity controls, or they can be addressed by documentation or approval processes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 28
□□ □ □□□ □□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □□□ □□□□□?
A. □□ □□
B. □□□ □□□ □□
C. □□□ □□ □□□□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)
A self-checking digit is the most effective accuracy control for entry of a valid numeric part number. This method involves adding an extra digit at the end of every number which is calculated from the other digits. This digit is then used to check the accuracy of the entered number1. While hash totals, online review of description, and comparison to historical order pattern can be used as accuracy controls, they are not as effective as a self-checking digit.

NEW QUESTION: 29
□□ □□□ □□□□ □□□□□ □□□□□□ □, □□□□ □□□□ □□□ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□□ □□
B. □□ □□□ □□□□ □ □□□
C. □□□□ □□
D. □□ □ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 30
IS □□□□ □□□□□ □□ □□ □□ □□□□ □□□ □□□ □□□□□□ □□□□ □ □ □□ □ □□□ □□□ □□□?
A. □□ □□ □□ □□
B. □□□□ □□ □□ □□
C. □□□□ □□ □□□□ □□
D. □□ □□
Answer: (SHOW ANSWER)
Scope creep is the uncontrolled expansion of a project's scope, which can result in delays, cost overruns, and quality issues. To mitigate the risk of scope creep, an IS auditor should

look for project change management controls, which are processes and procedures for managing changes to the project's scope, schedule, budget, and quality. Project change management controls ensure that changes are properly requested, approved, documented, communicated, and implemented. Source code version control, existence of an architecture review board, and configuration management are also important for software development, but they do not directly address the risk of scope creep.
References: ISACA Frameworks: Blueprints for Success, Project Management Institute: A Guide to the Project Management Body of Knowledge

NEW QUESTION: 31
□□ □□□ □□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □ □□□ □□□ IS □□□□□ □□□ □□ □□□ □□□ □□□ □□□□□. □□ □ □□ □□ □□□ □□ □ □□ □ □□□ □□□□?
A. □□□ □□
B. □□ □□ □□ □□□□(VLAN)
C. □□□
D. □□ □□
Answer: (SHOW ANSWER)
The best option to support the organization's objectives of protecting data confidentiality while transporting data is encryption. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm, so that only authorized parties can access the original data. Encryption protects the confidentiality of data in transit by preventing unauthorized interception, modification, or disclosure of the data. Encryption can also help comply with data privacy and security regulations, such as the GDPR and HIPAA.
The other options are not as effective as encryption in protecting data confidentiality while transporting data.
Cryptographic hashes are mathematical functions that generate a fixed-length output from an input, but they do not encrypt the data. Hashes are used to verify the integrity and authenticity of data, but they do not prevent unauthorized access to the data. Virtual local area network (VLAN) is a logical grouping of network devices that share the same broadcast domain, but they do not encrypt the data. VLANs can improve network performance and security by isolating traffic, but they do not protect the data from being intercepted or modified by external attackers. Dedicated lines are physical connections that provide exclusive access to a network or service, but they do not encrypt the data. Dedicated lines can offer higher bandwidth and reliability, but they do not guarantee the confidentiality of the data from being compromised by physical tampering or eavesdropping.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471

* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* Data Security and Confidentiality Guidelines - Centers for Disease Control and Prevention3
* Information Security | Confidentiality - GeeksforGeeks4

NEW QUESTION: 32
□□ □ □□□ □□□□ □□□ □ □□ □□ □□□□ □□ □□ □□□□□?
A. □□
B. □□ □□
C. □□
D. □□
Answer: B (LEAVE A REPLY)
A digital signature is a cryptographic technique that uses the sender's private key to generate a unique code for a message or document. The receiver can use the sender's public key to verify the authenticity and integrity of the message or document. A digital signature can prevent unauthorized change, as any modification to the message or document will invalidate the signature and alert the receiver of tampering.
References
What is a digital signature?
Digital Signature - an overview | ScienceDirect Topics
ISACA CISA Review Manual, 27th Edition, page 253

NEW QUESTION: 33
□□ □□ □□□□ □□ □□□ □□□ □□□□.
A. □□□□□ □□□□□ □□□□□.
B. □□□□□□ □□□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
A configuration management system is a process that establishes and maintains the consistency of a product's attributes throughout its life cycle. It helps to identify and control the functional and physical characteristics of a product, and to record and report any

changes to those characteristics. A configuration management system also supports the audit of the product to verify its conformance to requirements.
One of the key activities of a configuration management system is to define baselines for software. A baseline is a fixed reference point that serves as a basis for comparison and measurement. A baseline can be established for any configuration item, such as a requirement, a design document, a test plan, or a software component. A baseline helps to ensure that the software product meets its intended purpose and quality standards, and that any changes to the software are controlled and documented.
A configuration management system also supports other activities, such as tracking software updates, supporting the release procedure, and standardizing change approval, but these are not its primary purpose.
Therefore, the other options are incorrect.
References: : What is configuration management - Red Hat : Configuration Management | Definition, Importance & Benefits - ServerWatch

NEW QUESTION: 34
□□□ □□ □□(DLP) □□□ □□□□□□ □□ □□□ □□ □□□ □□□□□.
A. □□□□ □□ □□□□ □□.
B. □□ □□□□□ □□□□ □□ □□□□□□□.
C. □□□ □□□ □□□ □□□ □□□□□□ □□.
D. □□□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
DLP (Data Loss Prevention) toolsare designed toprevent unauthorized access, transfer, or leakage of sensitive data, especially byinsider threatsorunauthorized downloads.
* Preventing Unauthorized Downloads (Correct Answer - C)
* DLP solutionsblock or log attemptsto transfer sensitive files.
* Example:A DLP tool detects andblocks an employee from copying confidential data to a USB drive.
* Preventing Malware Installation (Incorrect - A, B)
* Antivirus and endpoint protection tools, not DLP, handle malware threats.
* Preventing Corrupt Data Transmission (Incorrect - D)
* DLP focuses ondata protection, not detecting corrupt files.
References:
* ISACA CISA Review Manual
* NIST 800-53 (Data Protection Controls)
* CIS (Center for Internet Security) DLP Best Practices

NEW QUESTION: 35
□□□ □□ IS □□ □□□ □□ □□□ □□□□□?

A. □□ □□□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □□□ □□□□ □□□ □□.
B. □□□ □□ □□ □ □□ □□ □□□ □□□□ □□□ □□□□□ □□□□□.
C. □□ □□ □□ □ □□□ □□ □□□ □□□ □□□ □□□□□.
D. □□□ □□ □□ □ □□ □□□ □□□□ □□ □□□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Theprimary roleof an internalIS audit functionis to provideindependent assuranceonrisk management, internal controls, and governance processes.
* Option A (Incorrect):While audits may identifycontrol improvements, they donot initiate changes; management is responsible for implementation.
* Option B (Incorrect):Compliance audits arepartof IS auditing, but the main focus isassurance on risk and controls, not just compliance.
* Option C (Incorrect):Best practices and standards reviews are useful, but theydo not definethecore objectiveof an internal audit.
* Option D (Correct):The internal audit function'smain goalis toassess and assurethe effectiveness of an organization'srisk management and internal controls.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Coversaudit objectives, assurance functions, and risk management.

NEW QUESTION: 36
□□□□□□□ □□□□ □□ □□□□ □□□□ □ □□□□□. □□ □□ □ □□ □□ □ □□□ □□ □□ □□□□ □□□□□. □□□□ □□□□ □□□□ □□□□□ □□ □□ □□ □□□ □□□□□?
A. □□□□□ □ □□ □□
B. □□□ □□, □□ □□□ □□ □□
C. □ □□ □□□ □□ □□□ □□
D. □□ □□ □□□□ □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Reconciliation of total amounts by project is the best control to ensure that data is accurately entered into the job-costing system from spreadsheets. Reconciliation is a process of comparing two sets of data to identify any differences or discrepancies between them. By reconciling the total amounts by project from spreadsheets with those from the job-costing system, any errors or omissions in data entry can be detected and corrected.
Validity checks are controls that verify that data conforms to predefined formats or ranges. They can prevent entry of character data into numeric fields, but they cannot ensure that the numeric data is correct or complete.
Reasonableness checks are controls that verify that data is within expected or acceptable limits. They can detect outliers or anomalies in data, but they cannot ensure that the data matches the source. Display back of project detail after entry is a control that allows the user to review and confirm the data entered into the system. It can help reduce human

errors, but it cannot guarantee that the data is accurate or consistent with the source.
References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

NEW QUESTION: 37
□□ □□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□ □□ □□ □□□□□ □□ □□□□ □□□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
The planning phase is the stage of the internal audit process where contact is established with the individuals responsible for the business processes in scope for review. The planning phase involves defining the objectives, scope, and criteria of the audit, as well as identifying the key risks and controls related to the audited area. The planning phase also involves communicating with the auditee to obtain relevant information, documents, and data, as well as to schedule interviews, walkthroughs, and meetings. The planning phase aims to ensure that the audit team has a clear understanding of the audited area and its context, and that the audit plan is aligned with the expectations and needs of the auditee and other stakeholders.
The execution phase is the stage of the internal audit process where the audit team performs the audit procedures according to the audit plan. The execution phase involves testing the design and operating effectiveness of the controls, collecting and analyzing evidence, documenting the audit work and results, and identifying any issues or findings. The execution phase aims to provide sufficient and appropriate evidence to support the audit conclusions and recommendations.
The follow-up phase is the stage of the internal audit process where the audit team monitors and verifies the implementation of the corrective actions agreed upon by the auditee in response to the audit findings. The follow-up phase involves reviewing the evidence provided by the auditee, conducting additional tests or interviews if necessary, and evaluating whether the corrective actions have adequately addressed the root causes of the findings. The follow-up phase aims to ensure that the auditee has taken timely and effective actions to improve its processes and controls.
The selection phase is not a standard stage of the internal audit process, but it may refer to the process of selecting which areas or functions to audit based on a risk assessment or an annual audit plan. The selection phase involves evaluating the inherent and residual risks of each potential auditable area, considering the impact, likelihood, and frequency of those risks, as well as other factors such as regulatory requirements, stakeholder expectations, previous audit results, and available resources. The selection phase aims to

prioritize and allocate the audit resources to those areas that present the highest risks or opportunities for improvement.
Therefore, option A is the correct answer.
References:
* Stages and phases of internal audit - piranirisk.com
* Step-by-Step Internal Audit Checklist | AuditBoard
* Audit Process | The Office of Internal Audit - University of Oregon

NEW QUESTION: 38
□□ □ □□□(PKI) □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□□□ □ □□ □□□□ □□□□
B. □□□□ □□□ □□□□ □□□□ □□ □□ □□ □□□□□□
C. □□□□(CA)□□ □□□ □□□□ □□□□
D. □□□□ □□□□ □□□□ □□□□ □□□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 39
□□□□□ □□□ □□ □□□□ □□□□ □□ □□ □ □□ □□ □□□□□?
A. □□ □□ □□
B. □□ □□ □□(SSL)
C. □□□ □□□□(IP) □□ □□
D. □□ □□ □□□
Answer: C (LEAVE A REPLY)
Internet Protocol (IP) address restrictions are used in a firewall to protect the entity's internal resources by allowing or denying access to specific IP addresses or ranges of IP addresses based on predefined rules.
Remote access servers, Secure Sockets Layers (SSLs), and failover services are not directly related to firewall protection, but rather to other aspects of network security, such as authentication, encryption, and availability. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.2: Network Security Devices and Technologies

NEW QUESTION: 40
□□□ HR □□□□□□□ □□□□ □□□□□ Infrastructure as a Service(IaaS) □□□ □□□□□□□□ □□□□. □□□ □□□□□□□ □□ □□ □□ □□□ □□ □□ □□ □ □□□□ □□□□?
A. □□□□ □□□□ □□ □□□
B. □□□□ □□□
C. □□ □□ □□□□
D. □□
Answer: (SHOW ANSWER)

The organization is primarily responsible for the security configurations of the deployed application's operating system when migrating its HR application to an Infrastructure as a Service (IaaS) model in a private cloud. This is because in an IaaS model, the cloud provider is responsible for the security of the underlying infrastructure that they lease to their customers, such as servers, storage, and networks, while the customer is responsible for the security of the areas of the cloud infrastructure over which they have control, such as operating systems, middleware, and applications. Therefore, the organization needs to ensure that the operating system is properly configured, patched, hardened, and monitored to protect the HR application from unauthorized access or malicious attacks.
The other options are not primarily responsible for the security configurations of the deployed application's operating system. The cloud provider's external auditor is not responsible for any security configurations, but rather for verifying and reporting on the cloud provider's compliance with relevant standards and regulations.
The cloud provider is responsible for the security of the underlying infrastructure, but not for the operating system or any software installed on it by the customer. The operating system vendor is responsible for providing updates and patches for the operating system, but not for configuring or securing it according to the customer's needs.
References:
* 11: What Is IaaS (Infrastructure As A Service)? - Forbes
* 12: What is Shared Responsibility Model? - Check Point Software
* 13: Who Is Responsible for Cloud Security? - Security Intelligence

NEW QUESTION: 41
□□ □□□ □□□□ □□ □ □□□ □□□□□?
A. □□ □□□ □□□ □□□□□
B. □□□ □□□ □□□ □□□ □□
C. □□ □□□ □ □□□□ □□□ □□
D. □□ □□□ □□□□ □□□□□□
Answer: D (LEAVE A REPLY)
Incremental backups are backups that only copy the data that has changed since the last backup, whether it was a full or incremental backup. The main reason to use incremental backups is to minimize the backup time and resources, as they require less storage space and network bandwidth than full backups. Incremental backups can also improve key availability metrics, such as recovery point objective (RPO) and recovery time objective (RTO), but that is not their primary purpose. Reducing costs associated with backups and increasing backup resiliency and redundancy are possible benefits of incremental backups, but they depend on other factors, such as the backup frequency, retention policy, and media type. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION: 42

□□□ □□ □□ □□ □□□ □□□□ □□ □□ □□□□ □□□ □ □□ □ □□ □□□ □□□□ □□□?

A. □□ □□□

B. □□ □□ □□

C. □□ □□ □□

D. □□ □□ □□

Answer: (SHOW ANSWER)

The correct answer is D. Maintenance procedures should be considered when examining fire suppression systems as part of a data center environmental controls review. Fire suppression systems are critical for protecting the data center equipment and personnel from fire hazards. Therefore, they should be regularly maintained and tested to ensure their proper functioning and compliance with safety standards. Maintenance procedures should include inspection, cleaning, replacement, and repair of the fire suppression system components, as well as documentation of the maintenance activities and results. Installation manuals, onsite replacement availability, and insurance coverage are not directly related to the fire suppression system performance and effectiveness, and therefore are not relevant for the audit review. References: CISA Review Manual (Digital Version)1, page 403.

NEW QUESTION: 43

□□ □ □□□ □□ □□(DLP) □□□ □□□□ □ □□ □□ □□□ □□ □□□ □□□□ □?

A. □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□

B. □□□ □□□ □□□ □□□□□□ □□ □□ □ □□ □□ □□ □□ □ □□

C. □□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□□

D. □□ □□□ □□□ □ □□ □□□□□ □□ □□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

The success of a DLP implementation relies heavily on accurately defining and configuring the policies and rule sets. These configurations ensure that the DLP tool effectively monitors and controls the movement of sensitive data within the organization, thereby preventing data loss.

References

* ISACA CISA Review Manual 27th Edition, Page 301-302 (Data Loss Prevention)

NEW QUESTION: 44

□□ □□ □ □□ □□□ □□ □□□□ □□□□ □□□ □□ □ □□ □□□□?

A. □□ □□ □□ □□ □□

B. □□ □□□ □□

C. □□ □□ □□

D. □□ □□ □□ □□

Answer: (SHOW ANSWER)

The best way to facilitate the legal process in the event of an incident is to preserve the chain of custody of the evidence. The chain of custody is a record of who handled, accessed, or modified the evidence, when, where, how, and why. The chain of custody helps to ensure the integrity, authenticity, and admissibility of the evidence in a court of law. The chain of custody also helps to prevent tampering, alteration, or loss of evidence that could compromise the investigation or the prosecution. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 45
□□ □□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□□□?
A. □□ □□ □□(BIA)
B. □□□□
C. □□□ □□
D. □□ □□ □□□□
Answer: (SHOW ANSWER)
Risk assessment is a mandatory part of the annual audit planning process, as it helps to identify and prioritize the areas that pose the highest risk to the organization's objectives and operations. Risk assessment involves analyzing the internal and external factors that affect the organization's risk profile, evaluating the likelihood and impact of potential events or scenarios, assessing the existing controls and mitigation strategies, and determining the residual risk level. Based on the risk assessment results, the IS auditor can allocate resources and schedule audits accordingly. A business impact analysis (BIA) is a process that identifies and evaluates the critical business functions and processes that could be disrupted by a disaster or incident, and estimates the potential impact on the organization's operations, reputation and finances. A BIA is not a mandatory part of the annual audit planning process, but it can be used as an input for risk assessment or as a subject for audit. Fieldwork is the phase of an audit where the IS auditor collects evidence to support the audit objectives and conclusions. Fieldwork is not part of the annual audit planning process, but it is part of each individual audit engagement. A risk control matrix is a tool that maps the risks identified in a risk assessment to the controls that mitigate them. A risk control matrix is not a mandatory part of the annual audit planning process, but it can be used as an output of risk assessment or as a tool for audit testing. References: CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.2: Audit Planning.

NEW QUESTION: 46
□□ □□□ □□□ □□□ □□ □□ □□□ □ □□ □□□ □□ □□ □□ □□ □□□□ □?
A. □□ □□
B. □□ □□

C. □□ □□

D. □□ □□

Answer: (SHOW ANSWER)

Segregation of duties is a fundamental concept in cybersecurity and information security. It refers to the practice of dividing critical tasks and responsibilities among different individuals or roles within an organization to reduce the risk of fraud, error, or unauthorized activities1. Segregation of duties is designed to prevent unilateral actions within an organization's workflow, which can result in damaging events that would exceed the organization's risk tolerance2.

There are different types of responses to risk associated with segregation of duties, depending on the level of risk and the cost-benefit analysis. Some of the common responses are:

Risk acceptance: This means acknowledging a risk and deciding to tolerate it without taking any corrective actions. This response is usually chosen when the risk is low or the cost of mitigation is too high3.

Risk mitigation: This means taking steps ahead of time to lessen the effects of a risk and make it less likely to happen. Some examples of mitigation strategies are making backup plans, setting up early warning systems, and staying away from high-risk areas or activities4.

Risk transference: This means shifting the negative impact of a risk and/or the responsibility for managing the risk response to a third party. Some examples of transference strategies are outsourcing, insurance, or contracts5.

Risk reduction: This means reducing the probability and/or severity of the risk below a threshold of acceptability. Some examples of reduction strategies are implementing controls, policies, or procedures to prevent or detect risks6.

Based on these definitions, the response to risk associated with segregation of duties that would incur the lowest initial cost is A. Risk acceptance. This is because risk acceptance does not require any additional resources or actions to address the risk. However, risk acceptance also implies that the organization is willing to bear the consequences of the risk if it occurs, which could be costly in the long run.

Therefore, the correct answer to your question is A. Risk acceptance.

NEW QUESTION: 47

□□□ □ □□□ □□□□ □□□□□ □□□□ □□ □□□ □□□ □□□□, □□ □ □ □ □□□ □□□□ □□ □□□ □□□?

A. □□ □□ □□□ □□ □□

B. □□□ □□□□□ □□□ □□□

C. □□□ □□□□□ □□

D. □□ □□□ □□□ □□-□□ □□

Answer: D (LEAVE A REPLY)

The most important part of a feasibility study is the economics1. A cost-benefit analysis of available products is crucial as it helps to understand the economic viability of the project1. It compares the costs of the project with the benefits it is expected to deliver, which is essential for making informed decisions1. Omitting this could lead to investments in hardware that may not provide the expected returns or meet the organization's needs.

References:

The Components of a Feasibility Study - ProjectEngineer

NEW QUESTION: 48

□□ □ □□□ □□ □□□ □□□□□ □□ □□□ □□□ □□□□□ □□ □□ □□□ □□□□□?

A. □□□□ □□ □□□□ □□ □□ □□ □□

B. 1□ □□ □ □□□□ □□□□ □□□□□.

C. 30□ □ □□ □□□ □□□□ □□□ □□

D. □□□□ □□□ □□□□ □□□ □□□□□ □□□ □ □□□ □□

Answer: A (LEAVE A REPLY)

The best strategy to optimize data storage without compromising data retention practices is to limit the size of file attachments being sent via email. This strategy can reduce the amount of storage space required for email messages, as well as the network bandwidth consumed by email traffic. File attachments can be large and often contain redundant or unnecessary information that can be compressed, converted, or removed before sending. By limiting the size of file attachments, the sender can encourage the use of more efficient formats, such as PDF or ZIP, or alternative methods of sharing files, such as cloud storage or web links. This can also improve the security and privacy of email communications, as large attachments may pose a higher risk of being intercepted, corrupted, or infected by malware.

References:

* Data Storage Optimization: What is it and Why Does it Matter?
* Data storage optimization 101: Everything you need to know

NEW QUESTION: 49

□□ □ □□ □□□ □□□ □□ □ □□□ □□□ □□□□□?

A. □□□ □□

B. □□ □□

C. □□ □□ □□
D. □□ □□ □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 50
□□ □□ □□ □□□ □□ □□□ □, □□□□ □□□ □□□□ □□ □□□ □□ □ □□ □□□ □□□?
A. □□ □□ □□□ □□□□□□ □□□ □□ □□□□ □□□□□.
B. □□ □□ □□□ □□□□ □□ □□ □□
C. □□ □□ □□□ □□ □□□□ □□ □□□ □□□□□
D. □□ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 51
□□□□ □□ □□□□□ □□□□ □□ □□ □□□ □□ □□□ □□□□□?
A. □□
B. □□□
C. □□□
D. □□
Answer: (SHOW ANSWER)
Secure code reviews as part of a continuous deployment program are preventive controls. Preventive controls are controls that aim to prevent or avoid undesirable events or outcomes from occurring, such as errors, defects, or incidents. Secure code reviews are activities that examine and evaluate the source code of a software or application to identify and eliminate any vulnerabilities, flaws, or weaknesses that may compromise its security, functionality, or performance. Secure code reviews as part of a continuous deployment program can help prevent or avoid security issues or incidents from occurring by ensuring that the code is secure and compliant before it is deployed to production. The other options are not correct types of controls for secure code reviews as part of a continuous deployment program, as they have different meanings and functions. Detective controls are controls that aim to detect or discover undesirable events or outcomes that have occurred, such as errors, defects, or incidents. Logical controls are controls that use software or hardware mechanisms to regulate or restrict access to IT resources, such as data, systems, or networks.
Corrective controls are controls that aim to correct or rectify undesirable events or outcomes that have occurred, such as errors, defects, or incidents. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 52
IS □□ □□□□ □□□ □□□□□ □ □□ □□□ □□ □□ □□□ □□□□□?
A. Agile □□

B. □□□□ □□
C. □□□□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
Risk-based auditing is an audit approach that focuses on the analysis and management of risk within an organization. Risk-based auditing helps identify and prioritize the areas or processes that pose the highest risk to the organization's objectives and allocate audit resources accordingly. Risk-based auditing also helps provide assurance and advisory services related to the organization's risk management processes and controls.
By using risk-based auditing, internal auditors can optimize the use of their audit resources and add value to the organization.
Agile auditing, continuous auditing, and outsourced auditing are not audit approaches that are most helpful in optimizing the use of IS audit resources. Agile auditing is a flexible and iterative audit methodology that adapts to changing circumstances and stakeholder needs. Continuous auditing is a method of performing audit activities on a real-time or near-real-time basis using automated tools and techniques. Outsourced auditing is a practice of contracting external auditors to perform some or all of the internal audit functions. These audit methods may have some advantages or disadvantages depending on the context and objectives of the audit, but they do not necessarily optimize the use of IS audit resources.

NEW QUESTION: 53
□□□□□ □□□ □□□ □□□□□□ □□□ □□ □ □□ □□□ □□ □□□□□?
A. □ □□□□□ □□□ □□□ □□ □□□□.
B. □□□□ □□ □□□ □ □□□□□□□.
C. □ □□□□□□ □□□ □□□ □□□ □□□□.
D. □ □□□□□□□ □□ □□□ □□ □□□ □□□□□ □□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 54
□□ □ □□□□□ □□□ □□□□□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □?
A. □□□□ □□ □□□□□ □□ □□
B. □□□□□□ □□□□ □□□ □□ □□ □□
C. □□□□ □□□ □□□□ □□ □□ □□
D. □□ □□ □□□□ □□□ □□□□□□ □□□ □□
Answer: D (LEAVE A REPLY)
Involving the application owner early in the audit planning process is the best way to contribute to the quality of an audit of a business-critical application. The application owner has a deep understanding of the application and its business context, which can provide valuable insights for the audit. Early involvement can also help ensure that the audit is

aligned with the business objectives and risks, and that any potential issues are identified and addressed promptly12.
References:
Business Critical Applications: An In-Depth Look
Framework for Audit Quality - IFAC

NEW QUESTION: 55
□□□□ □□ □□ IS □□□□ □□□□ □□□□ □□ □□□□ □□□□□□ □□□□ □□. □ □□□□ □□□□ □□ □□□□ □ □□□ □□ □ □□ □□□□?
A. □□□□□ □□□
B. □□□□ □□□
C. □□□ □□□□
D. □□□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The answer D is correct because the greatest concern for an IS auditor with the situation of business owners being removed from the project initiation phase is that the requirements may be incomplete. The project initiation phase is the first step in starting a new project, where the project's purpose, scope, objectives, and deliverables are defined and documented. The project initiation phase also involves identifying and engaging the key stakeholders who have an interest or influence in the project, such as sponsors, customers, users, or business owners.
Business owners are the individuals or entities who have the authority and responsibility to define the business needs and expectations for the project. They are also the primary beneficiaries of the project outcomes and benefits. Business owners play a crucial role in the project initiation phase, as they provide valuable input and feedback on the requirements and specifications of the project. Requirements are the statements that describe what the project should accomplish or deliver to meet the business needs and expectations. Requirements are essential for guiding the project planning, execution, monitoring, and closure phases.
If business owners are removed from the project initiation phase, it can result in incomplete or inaccurate requirements, which can have negative impacts on the project's quality, scope, time, cost, and risk. Some of the possible consequences of incomplete requirements are:
* Misalignment: The project may not align with the business strategy, vision, or goals, which can reduce its value or relevance.
* Confusion: The project team may not have a clear understanding of what the project should achieve or deliver, which can affect their performance or productivity.
* Rework: The project may need to undergo frequent changes or revisions to accommodate new or modified requirements, which can increase the time and cost of the project.

* Dissatisfaction: The project may not meet the expectations or satisfaction of the business owners or other stakeholders, which can affect their acceptance or support of the project.
* Failure: The project may not deliver the expected outcomes or benefits, which can affect its success or viability.
Therefore, an IS auditor should be concerned about the involvement and participation of business owners in the project initiation phase, as it affects the completeness and quality of requirements. An IS auditor should review the policies and procedures for stakeholder identification and engagement, verify that the business owners have adequate knowledge and skills to define their requirements, and test that the requirements are well-defined, documented, approved, and communicated.
References:
* Project Initiation: The First Step to Project Management [2023] * Asana
* Everything you need to know about the project initiation phase
* Project Initiation Phase - The Business Professor
* Project Initiation: A Guide to Starting a Project Right Way - Kissflow

NEW QUESTION: 56
□□ □ □□ □□ □□□□□ □□□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□
B. □□ □□ □□
C. □□□ □□ □
D. □□ □□ □□ □
Answer: D (LEAVE A REPLY)
The best performance indicator for the effectiveness of an incident management program is the incident resolution meantime. This is the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. The incident resolution meantime reflects how quickly and efficiently the incident management team can restore normal service and minimize the impact of incidents on the business operations and customer satisfaction.
The average time between incidents (option A) is not a good performance indicator for the effectiveness of an incident management program, as it does not measure how well the incidents are handled or resolved. It only shows how frequently the incidents occur, which may depend on various factors beyond the control of the incident management team, such as the complexity and reliability of the systems, the security threats and vulnerabilities, and the user behavior and expectations.
The incident alert meantime (option B) is the average time it takes to detect and report an incident. While this is an important metric for measuring the responsiveness and awareness of the incident management team, it does not indicate how effective the incident management program is in resolving the incidents and restoring normal service.
The number of incidents reported (option C) is also not a good performance indicator for the effectiveness of an incident management program, as it does not reflect how well the

incidents are handled or resolved. It only shows how many incidents are identified and recorded, which may vary depending on the reporting channels, tools, and procedures used by the incident management team and the users.
Therefore, option D is the correct answer.
References:
* Incident Management: Processes, Best Practices & Tools - Atlassian
* What is backup and disaster recovery? | IBM

NEW QUESTION: 57
IS □□□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□□. □□□ □□□□ □ □□ □□□ □□□ □□□□□ □□ □□ □□□ □□ □□□ □□□ □□□□.
A. □□□ □□ □□□ □□ □□□□ □□□□□.
B. □□□ □□□ □□□□□ □□□ □□□ □□□□□□□.
C. □□ □□□□□□□ □□□ □□□□ □□□ □□□ □□□□□.
D. □□ □□□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
This is because analyzing the data against predefined specifications is a method of data quality assessment that can help the organization achieve a reasonable level of data quality. Data quality assessment is the process of measuring and evaluating the accuracy, completeness, consistency, timeliness, validity, and usability of the data. Predefined specifications are the criteria or standards that define the expected or desired quality of the data. By comparing the actual data with the predefined specifications, the organization can identify and quantify any gaps, errors, or deviations in the data quality, and take corrective actions accordingly12.
Reviewing data against data classification standards (A) is not the best answer, because it is not a method of data quality assessment, but rather a method of data security management. Data classification standards are the rules or guidelines that define the level of sensitivity and confidentiality of the data, and determine the appropriate security and access controls for the data. For example, data can be classified into public, internal, confidential, or restricted categories. Reviewing data against data classification standards can help the organization protect the data from unauthorized or inappropriate use or disclosure, but it does not directly improve the data quality3.
Outsourcing data cleansing to skilled service providers (B) is not the best answer, because it is not a recommendation to help the organization achieve a reasonable level of data quality, but rather a decision to delegate or transfer the responsibility of data quality management to external parties. Data cleansing is the process of detecting and correcting any errors, inconsistencies, or anomalies in the data. Skilled service providers are third-party vendors or contractors that have the expertise and resources to perform data cleansing tasks. Outsourcing data cleansing to skilled service providers may have some benefits, such as cost savings, efficiency, or scalability, but it also has some risks, such as loss of control, dependency, or liability4.

Consolidating data stored across separate databases into a warehouse is not the best answer, because it is not a method of data quality assessment, but rather a method of data integration and storage. Data integration is the process of combining and transforming data from different sources and formats into a unified and consistent view. Data warehouse is a centralized repository that stores integrated and historical data for analytical purposes. Consolidating data stored across separate databases into a warehouse can help the organization improve the availability and accessibility of the data, but it does not necessarily improve the data quality.

NEW QUESTION: 58
□□□□ □□□ □□□ □□ □□(DLP) □□□ □□□□ □□□□. □□ □ □□ □□ □□ □□ □□ □□ □□□ □□□ □ □□ □□□□□□?
A. □□ □□ □ □□ □□ □□ □□
B. □□□ □□ □□ □□
C. □□□ □□□□ □□ □□
D. □□ □□□ □ □□
Answer: (SHOW ANSWER)
To reduce false positive alerts, it is essential to carefully configure a limited set of rules tailored to the organization's specific data loss prevention needs. This ensures that the DLP tool accurately identifies true positives and reduces the occurrence of false alarms.
References
* ISACA CISA Review Manual 27th Edition, Page 304-305 (DLP Tool Configuration)

NEW QUESTION: 59
□ □□□ IT □□ □□ □□□ □□□□□□. □□ □□ □□□□ □□ □ □□ □□□ □□ □□□□ □□□□□ □□□ □ □□□□?
A. IT □□□
B. □□□ □□
C. □□ □□
D. □□□□□□ □□
Answer: C (LEAVE A REPLY)
Segregation of duties (SOD) is a core internal control and an essential component of an effective risk management strategy. SOD emphasizes sharing the responsibilities of key business processesby distributing the discrete functions of these processes to multiple people and departments, helping to reduce the risk of possible errors and fraud1.
SOD is especially important in IT security, where granting excessive system access to one person or group can lead to harmful consequences, such as data breaches, identity theft, or bypassing security controls2. SOD breaks IT-related tasks into four separate function categories: authorization, custody, recordkeeping, and reconciliation1. Ideally, no one person or department holds responsibility in multiple categories.

In a role-based environment, where access privileges are granted based on predefined roles, it is important to ensure that the roles are designed and assigned in a way that supports SOD. For example, the person who develops an application should not also be the one who tests it, deploys it, or maintains it.
Therefore, an application developer should not be assigned the roles of IT operator, system administration, or database administration, as these roles may conflict with their development role and create opportunities for misuse or abuse of the system. The only role that may be assigned to an application developer without violating SOD is emergency support, which is a temporary role that allows the developer to access the system in case of a critical issue that requires immediate resolution3. However, even this role should be granted with caution and monitored closely to ensure compliance with SOD policies.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, page 2824
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID
1066692
* Hyperproof Blog, Segregation of Duties: What it is and Why it's Important1
* Advisera Blog, Segregation of duties in your ISMS according to ISO 27001 A.6.1.23

NEW QUESTION: 60
□□□ □□□□ □□□ □□ □□□□ □□□□□ □□ □□ □□ □□□ □□□ □□□ □□□□ □□□□. □□□ □□□ □□□□ □□□ □□□ □□□ □□□□. □□ □ □ □ □□ □□□ □□ □ □□□ □□□□□?
A. □□□□ □□□□□□ □□□ □□□ □ □□□□.
B. □□□□ □□□ □□□□ □ □ □□□□.
C. □□□□ □□□□ □□ □□□ □ □ □□□□.
D. □□□□ □□ □□□□ □□□□□□ □□□ □ □□□□.
Answer: C (LEAVE A REPLY)
The greatest risk associated with having most users with administrator access to an externally facing system containing sensitive data is that users can make unauthorized changes to the system or the data, which could compromise the integrity, confidentiality, and availability of the system and the data. Users can export application logs, view sensitive data, and install open-licensed software are also risks, but they are not as severe as unauthorized changes. References: ISACA CISA Review Manual 27th Edition Chapter 4

NEW QUESTION: 61
□□ □□□□ □□ □□ □□□□□□□ □□□□□ □□□□ □□□ □□□□□ □□□ □ IS □□□□ □□ □□□ □□□□ □□□.
A. □□□□□□ □□□ □□ □□ □□□□□.
B. □□ □□□□ □□ □□□□□ □□ □□□ □□□□.

C. □□ □□□□□□□ □ □□□ □□□□ □□□□□.
D. □ □□□□□□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
A database conflict occurs when the same data is modified at two separate servers, such as a customer database and a remote call center database, and the changes are not consistent with each other. For example, if a customer updates their phone number at the customer database, and a call center agent updates the same customer's address at the remote call center database, there is a conflict between the two updates. Database conflicts can cause data inconsistency, corruption, or loss if they are not detected and resolved properly.
Two-way replication is a process of synchronizing data between two databases, so that any changes made in one database are reflected in the other database, and vice versa. Two-way replication can improve data availability, performance, and scalability, but it also increases the risk of database conflicts. Therefore, when assessing a proposed project for the two-way replication of a customer database with a remote call center, the IS auditor should ensure that database conflicts are managed during replication. This means that the project should have a clear and effective strategy for:
* Preventing or minimizing database conflicts by using techniques such as locking, timestamping, or partitioning.
* Detecting or identifying database conflicts by using tools such as triggers, logs, or alerts.
* Resolving or handling database conflicts by using methods such as priority-based, rule-based, or user- based resolution.
The other possible options are:
* B. end users are trained in the replication process: This is not a relevant or important factor for the IS auditor to ensure when assessing a proposed project for the two-way replication of a customer database with a remote call center. End users are not directly involved in the replication process, and they do not need to have detailed knowledge or skills about how replication works. The replication process should be transparent and seamless to the end users, and they should only interact with the data through their applications or interfaces.
* C. the source database is backed up on both sites: This is not a sufficient or necessary factor for the IS auditor to ensure when assessing a proposed project for the two-way replication of a customer database with a remote call center. Backing up the source database on both sites can provide some level of data protection and recovery, but it does not address the issue of database conflicts that can occur during replication. Moreover, backing up the source database on both sites may not be feasible or efficient, as it may consume more storage space and network bandwidth, and introduce more complexity and overhead to the replication process.
* D. user rights are identical on both databases: This is not a critical or relevant factor for the IS auditor to ensure when assessing a proposed project for the two-way replication of a customer database with a remote call center. User rights are the permissions or privileges

that users have to access or modify data in a database. User rights do not directly affect the occurrence or resolution of database conflicts during replication. User rights may vary depending on the role or function of the users in different databases, and they should be defined and enforced according to the security policies and requirements of each database.

NEW QUESTION: 62
□□□□ □□□ □□ □□□□ □□□□□ □□□ □□ □□□ □ □□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□ □□ □□
B. □□□ □□
C. □□ □□□□ □□
D. □□□ □□ □□(SLA)
Answer: B (LEAVE A REPLY)
Data classification is the first consideration when deciding whether data should be moved to a cloud provider for storage because it determines the level of protection and security required for the data. Data classification also helps to identify the legal and regulatory requirements that apply to the data, such as privacy, retention and disposal policies. Data storage costs, vendor cloud certification and service level agreements (SLAs) are important factors to consider, but they are secondary to data classification. References: CISA Review Manual (Digital Version) 1, Chapter 5, Section 5.3.2

NEW QUESTION: 63
IT □□ □□□□ □□ □□ □□□ □□□□□.
A. IT □□□□ □□□□□ □□
B. IT □□□ □□ □□
C. IT □□ □ □□□ □□
D. IT □□ □□□□□□□ □□ □□□□
Answer: B (LEAVE A REPLY)
An IT balanced scorecard is primarily used for measuring IT strategic performance. An IT balanced scorecard is a framework that translates the IT strategy into measurable objectives, indicators, targets, and initiatives across four perspectives: financial, customer, internal process, and learning and growth. An IT balanced scorecard helps to monitor and

evaluate how well the IT function is delivering value to the organization, achieving its strategic goals, and improving its capabilities and competencies. The otheroptions are not the primary uses of an IT balanced scorecard, because they either focus on specific aspects of IT rather than the overall performance, or they are not directly related to the IT strategy. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.3

NEW QUESTION: 64
□□ □□□□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□□ □□
B. □□ □□ □□
C. □□ □□□□ □□□ □□□□ □
D. □□ □□□ □□□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
□□ □ □□□ □□ □□□□□ □□ □□ □□□□□ □□□□ □ □□ □□□ □□ □□ □□□?
A. □□□□□ □□□□ □□ □□□□□ □□□ □□□□□□□.
B. □□□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□□.
C. □□□ □□□ □□ □□□ □□□ □□□ □□□ □□□□□ □□ □□□□□□.
D. □□□□□ □□□ □□□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)
A benefits realization process is a systematic way of identifying, defining, planning, tracking and realizing the benefits from a project or program. Benefits are the measurable improvements that result from the delivery of project outputs and outcomes. Benefits realization management (BRM) is the practice of ensuring that benefits are derived from outputs and outcomes.
One of the best practices for BRM is to select metrics for the project before it begins. Metrics are the indicators that measure the performance and value of the project and its benefits. By selecting metrics in advance, the project team can align the project objectives with the expected benefits, establish a baseline for comparison, and monitor and evaluate the progress and results of the project. Metrics also help to communicate the value of the project to stakeholders and justify the investment.
The other options are not as effective as selecting metrics before the project begins. Project budget is an important factor for BRM, but it does not enable the benefits realization process by itself. It only reflects the costs of executing the project and delivering the solution, not the benefits or value that are expected from them. Estimates of business benefits are useful for planning and forecasting, but they are not sufficient for BRM. They need to be validated by actual data and evidence from similar projects or other sources. Metrics are evaluated after the project has been implemented, but this is only one part of the benefits realization process. BRM requires continuous monitoring and evaluation

throughout the project life cycle and beyond, to ensure that benefits are sustained and optimized.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 3261
PMI, Benefits Realization Management: A Practice Guide, 20192
APM, What is benefits management and project success?, 20213

NEW QUESTION: 66
□□□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□□□ □□ □□ □ □□ □ □□ □□□ □□□□ □□ □□□□?
A. □□□□ □□□
B. □□□ □□□□ □□ □□
C. □□□□ □□ □□□ □□
D. □□□□□ □□□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
□□□ □□ □□□ □□□ □□□□□□□ □□□□ □□ □□□ □□□□ □□□□□ □ □ □□□ □□□□□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□?
A. □□ □□ □□□
B. □□□□ □□ □□
C. □□□□ □3□ □□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
AChange Approval Board (CAB)ensures thatall necessary testing and rollback planshave been reviewed before deployment.
* Option A (Correct):ACABensures thatchanges are reviewed, tested, and approved, minimizing risks before an application is deployed. This includes confirming thatrollback plans are in place.
* Option B (Incorrect):Standardized change requestsare important but donot guarantee review and approvalby management and stakeholders.
* Option C (Incorrect):Third-party approvalmay be useful, but internalgovernance and control via a CABis more comprehensive.
* Option D (Incorrect):Secure code reviewshelp identify vulnerabilities, but they donot confirm proper deployment and rollback procedures.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coverschange management and deployment best practices.

NEW QUESTION: 68

□□□ □□□ □□ □□ □□□□□ □□□ □ IS □□□□ □□ □□ □□□ □□□ □ □ □□ □□□□□?

A. □ □□ □□□□ □□

B. □□ □□□ □□ □□

C. □□ □□ □□

D. □□ □□

Answer: D (LEAVE A REPLY)

Evidence collection is the process of identifying, acquiring, preserving, and documenting digital evidence from various sources, such as computers, networks, mobile devices, or cloud services, that can be used to support the investigation and prosecution of cybercrimes. Evidence collection is an IS auditor's primary focus when evaluating the response process for cybercrimes, because it determines the quality and validity of the evidence that can be used to prove or disprove the facts of the case, identify the perpetrators, and recover the losses. Evidence collection should follow the standards and best practices for digital forensics, such as ISO /IEC 270371, which provide guidelines for ensuring the integrity, authenticity, reliability, and admissibility of the evidence2.

The other possible options are:

* A. Communication with law enforcement: This is the process of reporting, cooperating, and coordinating with law enforcement agencies that have the jurisdiction and authority to investigate and prosecute cybercrimes. Communication with law enforcement is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Communication with law enforcement depends on the legal and regulatory requirements, the nature and severity of the incident, and the organizational policies and procedures. Communication with law enforcement should be done after evidence collection, to avoid compromising or contaminating the evidence3.
* B. Notification to regulators: This is the process of informing and updating the relevant regulatory bodies or authorities that oversee or supervise the organization's activities or industry sector about the cybercrime incident. Notification to regulators is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Notification to regulators depends on the legal and regulatory requirements, the nature and impact of the incident, and the organizational policies and procedures. Notification to regulators should be doneafter evidence collection, to avoid disclosing sensitiveor confidential information4.
* C. Root cause analysis: This is the process of identifying and analyzing the underlying factors or causes that led to or contributed to the cybercrime incident. Root cause analysis is an important aspect of the response process for cybercrimes, but it is not an IS auditor's primary focus when evaluating it. Root cause analysis helps to prevent or mitigate future incidents, improve security controls and processes, and learn from mistakes. Root cause analysis should be done after evidence collection, to avoid interfering with or affecting theinvestigation5.

NEW QUESTION: 69
□□ □□ □□ □□ IS □□□□ □□□□ □□ □□(BIA)□ □□□□ □□□□ □□ □□ □□□. □□□□ □□ □□□ □□□□ □□□.
A. □□ □□ □□(BIA)□ □□□□□.
B. □□□□□ □□ □□□□ □□□□□.
C. □□ □□ □□ □□□ □□□ □□□ □□□□□.
D. □□□□ □□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The first step that an IS auditor should take when finding that a business impact analysis (BIA) has not been performed is to evaluate the impact on current disaster recovery capability. A BIA is a process that identifies and analyzes the potential effects of disruptions to critical business functions and processes. A BIA helps determine the recovery priorities, objectives, and strategies for the organization. Without a BIA, the disaster recovery plan may not be aligned with the business needs and expectations, and may not provide adequate protection and recovery for the most critical assets and activities. Therefore, an IS auditor should assess how the lack of a BIA affects the current disaster recovery capability and identify any gaps or risks that need to be addressed.
Performing a BIA, issuing an intermediate report to management, and conducting additional compliance testing are not the first steps that an IS auditor should take when finding that a BIA has not been performed.
These steps may be done later in the audit process, after evaluating the impact on current disaster recovery capability. Performing a BIA is not the responsibility of the IS auditor, but of the business owners and managers. Issuing an intermediate report to management may be premature without sufficient evidence and analysis. Conducting additional compliance testing may not be relevant ornecessary without a clear understanding of the disaster recovery requirements and objectives.

NEW QUESTION: 70
□□ □□ □□ □ □□□□ □□□ □□(BCP)□ □□□□□ □□□□□ □□ □□ □□ □ □□ □□ □ □□□□□?
A. □ □□ □□□ □□ □□□□ □□□ □□□□□.
B. □□ □□□ □□□ □□□□□ □□ □□ □□□ □□□□□□.
C. □□ □□ □□□ □□□□□ □□□□□□□.
D. □□ □□□□□ □□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The best way to ensure that business continuity plans (BCPs) will work effectively in the event of a major disaster is to involve staff at all levels in periodic paper walk-through exercises. This means that the BCPs are tested and validated by the people who will execute them in a real situation, and any gaps, errors, or inconsistencies can be identified and corrected. Paper walk-through exercises are also a good way to raise awareness and

train staff on their roles and responsibilities in a BCP scenario, as well as to evaluate the feasibility and effectiveness of the recovery strategies1.
The other options are not the best ways to ensure that BCPs will work effectively, because they do not involve testing or validating the plans. Preparing detailed plans for each business function is important, but it does not guarantee that the plans are realistic, practical, or aligned with the overall business objectives and priorities2. Regularly updating business impact assessments is also essential, but it does not ensure that the BCPs are aligned with the current business environment and risks2. Making senior managers responsible for their plan sections is a good way to assign accountability and authority, but it does not ensure that the plan sections are coordinated and integrated with each other2.
References:
* Best Practice Guide: Business Continuity Planning (BCP)3
* Best Practices for Creating a Business Continuity Plan1
* Business Continuity Plan Best Practices

NEW QUESTION: 71
□□ □ □□□ □□ □□□ □□ □□□□□ □□□ □ □□ □□ □□□□□?
A. □□□
B. □□□
C. □□□ □□
D. □□□
Answer: (SHOW ANSWER)
The best guard against the risk of attack by hackers is encryption. Encryption is the process of transforming data into an unreadable format using a secret key or algorithm. Encryption can protect data in transit and at rest from unauthorized access, modification, or disclosure by hackers. Encryption can also ensure the authenticity and integrity of data by using digital signatures or hashes.
Tunneling, message validation, and firewalls are not the best guards against the risk of attack by hackers.
Tunneling is a technique that encapsulates one network protocol within another to create a secure connection between two endpoints. Message validation is a process that verifies the format, content, and origin of a message before accepting it. Firewalls are devices or software that filter network traffic based on predefined rules. These controls may help reduce the exposure or impact of hacker attacks, but they do not provide the same level of protection as encryption.

NEW QUESTION: 72
□□□ □□□□ □□□□ □□ □□□ □□□□□ □□□ □□ □□□□□ □□ □ □□□ □□□□ □□□ □□□□ □□□□. □ □□□□□□ □□□□ □□ □□ □ □□ □□□ □□ □□□□□?
A. □□□ □□□ □□

B. □□□ □□
C. □□ □□ □□
D. □□ □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
□□□□ □□ □□ □□□□ □□□□ □□□ □ □□□ □□ □ □□□ □□□ □ □□ □ □ □ □□□□□?
A. □□□ □□□ □□□□(XSS)
B. □□□ □□
C. □□□□
D. □□□ □□ □□□□ □□□
Answer: C (LEAVE A REPLY)
Social engineering is the manipulation of people to perform actions or divulge confidential information. It is a common technique used by attackers to gain unauthorized access to systems or data. Employees who use public social networking sites may be vulnerable to social engineering attacks, such as phishing, baiting, or pretexting, which pose the greatest risk to the organization's security. The other options are not as serious as social engineering, as they relate to web application vulnerabilities, intellectual property rights, and reputation management, which are less likely to compromise the organization's assets or operations. References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.3 Security Awareness Training1

NEW QUESTION: 74
IS □□□□ □□□ □□□□ □□ □□□ □□□ □□□□ □□□ □□ □□□ □□(BCP) □ □□ □□□□□ □□□□ □□□□ □□□□ □□□ □□□□□□. □□□□ □□□ □ □ □□□ □□ □ □□ □□□□?
A. BCP□ □□ □□□□□□□□ □□□□□.
B. □□□□ □□□ □□□ □□□□□.
C. □□□□□ □□□□ □□□□ □□ □□□ □□□□□.
D. BCP□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
This is because the auditor's primary objective is to evaluate the adequacy and performance of the business continuity plan (BCP) in ensuring the continuity and resilience of the organization's critical functions and processes during a disruption. The auditor should review the actual results and outcomes of the business response, such as the recovery time, recovery point, service level, customer satisfaction, and incident management, and compare them with the predefined objectives and criteria of the BCP. The auditor should also identify and analyze any gaps, issues, or lessons learned from the business response, and provide recommendations for improvement12.

Answer A. Confirm the BCP has been recently updated. is not the best answer, because it is not directly related to the auditor's course of action. Confirming the BCP has been recently updated is a part of the audit planning and scoping process, not the audit execution or reporting process. The auditor should confirm the BCP has been recently updated before conducting the audit, not after revealing that a simulation test has not been performed. Moreover, confirming the BCP has been recently updated does not provide sufficient evidence of the effectiveness of the business response12.
Answer C. Raise an audit issue for the lack of simulated testing. is not the best answer, because it is not relevant to the auditor's course of action. Raising an audit issue for the lack of simulated testing is a part of the audit reporting and follow-up process, not the audit execution or evaluation process. The auditor should raise an audit issue for the lack of simulated testing after reviewing the effectiveness of the business response, not before or instead of doing so. Furthermore, raising an audit issue for the lack of simulated testing does not address the root cause or impact of the problem, nor does it provide any constructive feedback or guidance for improvement12.
Answer D. Interview staff members to obtain commentary on the BCP's effectiveness. is not the best answer, because it is not sufficient to guide the auditor's course of action. Interviewing staff members to obtain commentary on the BCP's effectiveness is a part of the audit evidence collection and analysis process, not the audit evaluation or conclusion process. The auditor should interview staff members to obtain commentary on the BCP's effectiveness as one of the sources of information, not as the only or main source of information. Additionally, interviewing staff members to obtain commentary on the BCP's effectiveness may be subjective, biased, or incomplete, and may not reflect the actual performance or outcomes of the business response12.
References:
Business Continuity Management Audit/Assurance Program
Business Continuity Plan Testing: Types and Best Practices

NEW QUESTION: 75
□□ □ IS □□ □□□□□ □□ □□ □□□ □□ □□ □□□ □□□ □□□□ □□ □□ □□□?
A. □□□□
B. IT □□□□□
C. □□□□□□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
The audit charter is the document that defines the purpose, authority and responsibility of the IS audit function. It provides IS audit professionals with the best source of direction for performing audit functions, as it establishes the scope, objectives, reporting lines, independence, accountability and resources of the IS audit function. The IT steering committee is a governance body that oversees the strategic alignment, prioritization and

direction of IT initiatives, but it does not provide specific guidance for IS audit functions. The information security policy is a document that defines the rules and principles for protecting information assets in the organization, but it does not cover all aspects of IS audit functions. Audit best practices are general guidelines and recommendations for conducting effective and efficient audits, but they are not binding or authoritative sources of direction for IS audit functions. References: CISA Review Manual (Digital Version) 1, Chapter 1: Information Systems Auditing Process, Section 1.1: Audit Charter.

NEW QUESTION: 76
□□ □ □□□ □□□□□ □□□□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□□□ □□□□□ □□ □□□ □□□□□.
B. □□□□□□ □□□ □□ □□(SLA)□ □□□□□ □□□□□.
C. □□□□□ IT □□□□ □□ □□□ □□□ □□□ □□□□□.
D. □□□□□ □□ □□ □□(CSA) □□□ □□□□.
Answer: A (LEAVE A REPLY)
The most effective method to verify that a service vendor keeps control levels as required by the client is to conduct periodic on-site assessments using agreed-upon criteria. On-site assessments can provide direct evidence of whether the vendor's controls are operating effectively and consistently in accordance with the client's expectations and requirements. Agreed-upon criteria can ensure that the assessments are objective, relevant, and reliable. The other options are not as effective as on-site assessments in verifying the vendor's control levels. Periodically reviewing the SLA with the vendor can help monitor whether the vendor meets its contractual obligations and service standards, but it does not provide assurance of whether the vendor's controls are adequate or sufficient. Conducting an unannounced vulnerability assessment of vendor's IT systems can help identify any weaknesses or gaps in the vendor's security controls, but it may violate the terms and conditions of the vendor-client relationship or cause operational disruptions. Obtaining evidence of the vendor's CSA can provide some indication of whether the vendor's controls are self-monitored and reported, but it does not verify whether the vendor's controls are independent or accurate. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION: 77
□□□ IT □□□□□□ □□□□□ □□□□□ □ □, IS □□□□ □□ □ □□ □□ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□□□ □□□□ IT □□ □□ □□□ □□□□ □□□□□.
B. □□ □□ □□ □□ □□ □□□ □□□□□.
C. □□ □□, □□ □ □□□ □□□□□.
D. □□ □□ □□ □□□ □□□ □□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 78
□□ □ IS □□□□□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□□ □□ □ □ □□ □□□ □ □□ □□ □□□□□?
A. □□□ □□□ □□
B. □□□ □□ □□
C. □□□ □□□ □□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)
Data disposal controls are the measures that ensure that data are securely and permanently erased or destroyed when they are no longer needed or authorized to be retained. Data disposal controls support business strategic objectives by reducing the risk of data breaches, complying with data privacy regulations, optimizing the use of storage resources, and enhancing the reputation and trust of the organization1.
A media sanitization policy is a document that defines the roles, responsibilities, procedures, and standards for sanitizing different types of media that contain sensitive or confidential data. Media sanitization is the process of removing or modifying data on a media device to make it unreadable or unrecoverable by any means. Media sanitization can be achieved by various methods, such as overwriting, degaussing, encryption, or physical destruction2.
A media sanitization policy would provide an IS auditor with the greatest assurance that data disposal controls support business strategic objectives because it demonstrates that the organization has a clear and consistent approach to protect its data from unauthorized access or disclosure throughout the data life cycle. A media sanitization policy also helps the organization to comply with various data privacy regulations, such as the EU General Data Protection Regulation (GDPR), the US Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS), that require proper disposal of personal or sensitive data3.
The other options are not as effective as a media sanitization policy in providing assurance that data disposal controls support business strategic objectives. A media recycling policy is a document that defines the criteria and procedures for reusing media devices that have been sanitized or erased. A media recycling policy can help the organization to save costs and reduce environmental impact, but it does not address how the data are disposed of in

the first place4. A media labeling policy is a document that defines the rules and standards for labeling media devices that contain sensitive or confidential data. A media labeling policy can help the organization to identify and classify its data assets, but it does not specify how the data are sanitized or destroyed when they are no longer needed. A media shredding policy is a document that defines the methods and procedures for physically destroying media devices that contain sensitive or confidential data. A media shredding policy can be a part of a media sanitization policy, but it is not sufficient to cover all types of media devices or data disposal scenarios.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* Secure Data Disposal and Destruction: 6 Methods to Follow1
* Why (and How to) Dispose of Digital Data2
* What is Data Disposition? The Complete Guide3
* Data Disposition: What is it and why should it be part of your data retention policy?

NEW QUESTION: 79
IT □□□□□□ □□□ □□□ □□ □□□ □□□□□ □□□ □ □□□□□ □□ □□□ □□ □□□□□?
A. □□□□□(ROI) □□
B. □□□□ □□(EVA)
C. □□□ □□ □□
D. □□ □□ □□(BIA)
Answer: (SHOW ANSWER)
EVA is a project management technique that measures the performance of a project by comparing the actual work completed, the actual costs incurred, and the planned costs for the work scheduled. EVA can help determine if the project is on track, ahead of schedule, or behind schedule, and if the project is under budget, over budget, or on budget. EVA can also help forecast the final cost and schedule of the project based on the current performance.
References
ISACA CISA Review Manual, 27th Edition, page 255
18. Project Completion - Project Management - 2nd Edition
How to Measure Project Success | Smartsheet

NEW QUESTION: 80
□□□ □□□□□□ □□ □□ □□□□ □□□□ □□□□□ □□ □□□□. □□ □□□ □ □□ □□(BIA)□ □□ □□□□ □□□?
A. □□□ □□ □□□ □□□□ □□
B. □□ □ □□ 1□

C. □□□ □□ □□□ □□□□ □□
D. □□ □□□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 81
□□ □ □□□□ □□□□ □□□□ □□□□ □□ □□ □□(KPI)□ □□ □□□ □□□ □□?
A. □□ □□□ □□ □□□□ □□ □ □□ □□□ □□ □□□ □□ □ □□□ □□□.
B. □□□□ □□□□□ □□□□□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □□□□□.
C. □□□□ □□□□□ □□□□ □□□□□ □□□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The primary role of key performance indicators (KPIs) in supporting business process effectiveness is to enable conclusions about the performance of the processes and target variances for follow-up analysis. KPIs are measurable values that demonstrate how effectively an organization is achieving its key objectives. KPIs can help to monitor and evaluate the performance, quality, and efficiency of the business processes. KPIs can also help to identify areas for improvement and benchmark against best practices or industry standards. KPIs can also provide feedback and guidance for decision making and corrective actions. References:
* CISA Review Manual (Digital Version), Chapter 1, Section 1.3.21
* CISA Online Review Course, Domain 5, Module 2, Lesson 22

NEW QUESTION: 82
IS □□ □□□□ □□ □□ □□ □□□□ □□ □□ □□□ □□□ □□ □□ □□□ □□ □□ □□□□. IS □□ □□□□ □□□ □□□□ □□ □□□□□ □□□□ □□ □□ □ □ □ □ □□□□□?
A. □□□□□ □□□ □□□ □ □□□ □□
B. □□ □□ □□ □□ □□□ □□□ □□ □□ □□□
C. □□□ □□□□ □□ □□ □□□ □□□ □□ □□
D. □□ □□ □□□□ □□□ □□□ □□ □□□ □□
Answer: D (LEAVE A REPLY)
The IS audit manager should specifically review the detailed evidence of the successes and weaknesses of all contingency testing to substantiate the conclusions of the audit of the corporate disaster recovery test. This is because the detailed evidence can provide the audit manager with a clear and objective picture of how well the disaster recovery plan was executed, what issues or gaps were encountered, and what recommendations or actions were taken to address them. The detailed evidence can also help the audit manager to verify the accuracy, completeness, and validity of the audit findings, as well as to evaluate the adequacy and effectiveness of the disaster recovery controls.

The other options are not as specific or relevant as the detailed evidence of all contingency testing. Overviews of interviews between data center personnel and the auditor may provide some useful information, but they are not sufficient to substantiate the conclusions without supporting evidence from the actual testing. Prior audit reports involving other corporate disaster recovery audits may provide some benchmarking or comparison data, but they are not directly related to the current audit scope and objectives. Summary memos reflecting audit opinions regarding noted weaknesses may provide some high-level insights, but they are not enough to substantiate the conclusions without detailed evidence to back them up.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2411
Disaster Recovery Audit Work Program2

NEW QUESTION: 83
IS □□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□, □ □□□ □□□□ □□ □□ □□□□ □□□ □□□□□□. □□□ □□□ □□ □□□□□ □ □□□□. □□□ □ □□ □□□ □□ □ □□ □□□□?
A. □□□ □□□ □□□ □□
B. □□ □□ □ □□
C. □□□ □□ □ □□ □□
D. □□□ □□□□□ □□□□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
□□□□ □□□ □□□ □□ □□□ □□□□□□. □□ □□ □□□ □□□ □□□ □□ □□ □□ □□□□.
A. □□ □□.
B. □□ □□(QA).
C. □□ □□.
D. □□□□ □□.
Answer: (SHOW ANSWER)
A weakness in change management is the most likely cause of an incorrect version of source code being amended by a development team. Change management is the process of controlling and documenting changes to IT systems and software. It ensures that changes are authorized, tested, and implemented in a controlled manner. If change management is weak, there is a risk of using outdated or incorrect versions of source code, which can lead to errors, defects, or security vulnerabilities in the software.

NEW QUESTION: 85
□□□ □□□□□ □□□□ □□ □ □□□ □□□□□?
A. □□□□□ □□□□□ □□□□ □ □□□□.

B. □□□□□□ □□□ □□□□ □ □□□□.
C. □□□□ □□□ □□□□□ □□□ □□□ □□□□.
D. □□□□ □□□□ □□ □ □□□□.
Answer: (SHOW ANSWER)
The primary benefit of using one-time passwords is that an intercepted password cannot be reused, as it is valid only for a single login session or transaction. One-time passwords enhance the security of authentication by preventing replay attacks or password guessing. The other options are not the primary benefits of using one-time passwords. Security for applications can be automated with or without one-time passwords. Users may still have to memorize complex passwords or use a device or software to generate one-time passwords. Users can still be locked out of an account if they enter an incorrect or expired one-time password. References: CISA Review Manual (Digital Version), Chapter 6, Section 6.1

NEW QUESTION: 86
IS □□□□ □□ □□ □□ □□□□□ □□ □□□□ □□□□ □□□□ □□ □□□ □ □□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□□□ □□
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Audit findings should be communicated as early as possible to avoid misunderstandings, provide an opportunity for corrective action, and ensure transparency.
* Option A (Incorrect):The planning phase involves defining audit scope, objectives, and methodology, but findings are not yet available to discuss with management.
* Option B (Incorrect):The reporting phase formalizes audit results, but discussing issuesonlyat this stage may lead to delays in corrective action.
* Option C (Incorrect):The follow-up phase ensures that management has implemented corrective actions, but this occursafterthe initial discussion of findings.
* Option D (Correct):The fieldwork phase is when auditors activelygather evidence, analyze data, and identify issues. Discussing observationsduringthis phase allows for immediate clarification, validation, and resolution of misunderstandings before the final report.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Discusses audit engagement, reporting, and communication best practices.

NEW QUESTION: 87
□□ □□□□ □□ □□□ □□ □□□□ □□□□ □ □□□□ □□□ □□□ □□□□ □?

A. □□□ □□□□□□ □□ □□(RASP)
B. □□ □□ □□ □□□(DAST)
C. □□□ □□□□□□ □□ □□□(IAST)
D. □□ □□ □□ □□□(SAST)
Answer: (SHOW ANSWER)

NEW QUESTION: 88
□□ □ □□ □□ □□□□□ □□□□□ □□ □ □□□□ □□ □□□□□?
A. IT □□□□ □□□ □□□□ □ □□
B. □□□ □□□ □□ □ □□
C. □□ □□ □□ □□
D. □□ □□□□ □□□□ □□ □□ □□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 89
□□ □ □□ □□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□□ □□□
B. □□□ □□□ □□□□
C. □□□ □□□
D. □□□ □□
Answer: (SHOW ANSWER)
End-to-end encryption ensures that email content is encrypted during transmission and can only be decrypted by the intended recipient. This approach provides robust protection against interception and unauthorized access.
* Encryption of Corporate Network Traffic (Option A):This does not address email confidentiality once the email leaves the corporate network.
* Complex User Passwords (Option B):Enhances account security but does not ensure email confidentiality in transit.
* Digital Signatures (Option D):Ensures authenticity and integrity but does not encrypt the email content.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 90
□□ □ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □ □□□ □□□ □□□ □□□□ □□
B. □□ □ □□□ □□□ □□ □□□□ □□□ □□□□□□.
C. IT □□□□ □□□ □□□ □□ □□□ □□□□ □□□□□.
D. □□□ □□ □□□ □□ □□ □□ □□(RPO)□ □□□□□
Answer: A (LEAVE A REPLY)

The best reason to implement a data retention policy is to limit the liability associated with storing and protecting information. A data retention policy is a document that defines how long data should be kept by an organization and how they should be disposed of when they are no longer needed. A data retention policy should comply with the applicable laws and regulations that govern the data retention requirements and obligations of organizations, such as tax laws, privacy laws, or industry standards4. Implementing a data retention policy can help to limit the liability associated with storing and protecting information by reducing the amount of data that need to be stored and secured, minimizing the risk of data breaches or leaks, ensuring compliance with legal or contractual obligations, and avoiding potential fines or penalties for non- compliance5. The other options are less relevant or incorrect because:

* B. Documenting business objectives for processing data within the organization is not a reason to implement a data retention policy, as it is more related to data governance than data retention. Data governance refers to the policies, procedures, and controls that define how data are collected, used, managed, and shared within an organization. Data governance helps to ensure that data are aligned with business objectives and support decision making6.
* C. Assigning responsibility and ownership for data protection outside IT is not a reason to implement a data retention policy, as it is more related to data accountability than data retention. Data accountability refers to the identification and assignment of roles and responsibilities for data protection among different stakeholders within an organization. Data accountability helps to ensure that data are handled appropriately and securely by authorized parties7.
* D. Establishing a recovery point objective (RPO) for disaster recovery procedures is not a reason to implement a data retention policy, as it is more related to data backup than data retention. Data backup refers to the process of creating copies of data that can be restored in case of data loss or corruption. Data backup helps to ensure that data are available and recoverable in case of disaster8. RPO is a measure of the maximum amount of data that can be lost or acceptable in case of disaster9. References: Data Retention Policy - ISACA, Data Retention - ISACA, Data Governance - ISACA, Data Accountability - ISACA, Data Backup - ISACA, Recovery Point Objective - ISACA

NEW QUESTION: 91

□□□□□□ □□□□ □□□□ □□□□ □□□ □ □□ □□□ □□□ □□□□ □□ □ □ □□□ □□□ □□□□ □□□□.

A. □□ □□ □□□□ □□ □□.

B. □□ □□□ □□ □□□ □□□ □□□□□□.

C. □□ □□ □□□□ □□.

D. □□□ □□ □□.

Answer: (SHOW ANSWER)

The best way to determine whether programmers have permission to alter data in the production environment is by reviewing the access rights that have been granted. Access rights are permissions or privileges that define what actions or operations a user can perform on an information system or resource. By reviewing the access rights that have been granted to programmers, an IS auditor can verify whether they have been authorized to modify data in the production environment, which is where live data and applications are stored and executed. The access control system's log settings are parameters that define what events or activities are recorded by the access control system, which is a system that enforces the access rights and policies of an information system or resource. The access control system's log settings are not the best way to determine whether programmers have permission to alter data in the production environment, as they do not indicate what permissions or privileges have been granted to programmers. How the latest system changes were implemented is a process that describes how software updates or modifications are deployed to the production environment. How the latest system changes were implemented is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers. The access control system's configuration is a set of rules or parameters that define how the access control system operates and functions. The access control system's configuration is not the best way to determine whether programmers have permission to alter data in the production environment, as it does not indicate what permissions or privileges have been granted to programmers.

NEW QUESTION: 92
□□ □□□ □□□ □□□□ □□□ IS □□□□ □□□□ □□ □□□ IT □□□□ □□□ □□□ □□□□□□. □□□□□□ □□□ □□□□ □ □□ □□□ □□ □□ □□ □ □ □ □□□□?
A. IT □□ □ □□□□ □□ □□ □□ □□□
B. □□□□□ IT □□ □□□□ □□□
C. □□ □3□ IS □□ □□□
D. □□ □ □□ □□ IS □□ □□□
Answer: C (LEAVE A REPLY)
Recent third-party IS audit reports would be most helpful in determining the effectiveness of the IT governance framework of the target company. IT governance is a framework that

defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. A third-party IS audit is an independent and objective examination of an organization's IT governance framework by an external auditor.
Recent third-party IS audit reports can provide reliable and unbiased evidence of the strengths, weaknesses, and maturity of the IT governance framework of the target company. The other options are not as helpful as recent third-party IS audit reports, as they may not be as comprehensive, accurate, or current as external audits. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION: 93
□□ □□□ □□□ □ IS □□□□ □□ □□□□□□ □□ □□ □□□ □□□ □□□ □ □□ □□□□□ □ □□ □□ □□□ □□□ □□□ □□□ □□□ □□□□. □□□□ □ □□ □□□ □□ □□□?
A. □□ □□□□ □□ □□□ □□□□□□ □□□□ □□ □□□□□□□ □□□□□.
B. □□□□ □□□ □□□□□ □□□ □□□□□□ □□□□□.
C. □□ □□□□ □□ □□□□ □ □□□ □□□ □□□□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
When operational management informs the IS auditor that recent organizational changes have addressed previously identified risks and implementing the action plan is no longer necessary, the IS auditor should accept management's assertion and report that the risks have been addressed. However, it is essential to document this communication and ensure that there is evidence supporting management's claim. If there are any doubts or concerns, further investigation may be necessary. The auditor should not assume new risks without proper assessment or evidence1. References:
1(https://www.isaca.org/resources/isaca-journal/issues
/2016/volume-6/enhancing-the-audit-follow-up-process-using-cobit-5)

NEW QUESTION: 94
IS □□□□ □□□□□ □□□ □□□□ □□□□□ □□ □□□ □□ □□□ □□□ □□ □□□□□□. □□□□ □□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□□ □□□ □□□□□□□ □□□□□.
B. □□□□ □□□ □□□□ □□ □□ □□
C. □□□□ □□□ □□ □□□ □□□□□□□.
D. □□ □□□ □□□□ □□□□□□□ □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
This means that the organization should obtain the source code from the escrow agent and compare it with the current version of the application that they are using. The organization should then identify and apply any changes or updates that are missing or different in the escrow version, so that it matches the current version.

This way, the organization can ensure that they have a complete and accurate copy of the source code that reflects their current needs and requirements.
Bringing the escrow version up to date can help the organization to avoid or reduce the risks and costs associated with using an outdated or incompatible version of the source code. For example, an older version of the source code may have bugs, errors, or vulnerabilities that could affect the functionality, security, or performance of the application. An older version of the source code may also lack some features, enhancements, or integrations that could improve the usability, efficiency, or value of the application. An older version of the source code may also not comply with some standards, regulations, or contracts that could affect the quality, reliability, or legality of the application1.
The other options are not as good as bringing the escrow version up to date for the organization. Option A, analyzing a new application that meets the current requirements, is a possible option but it may be more time- consuming, expensive, and risky than updating the existing application. The organization may have to go through a complex and lengthy process of selecting, acquiring, implementing, testing, and migrating to a new application, which could disrupt their operations and performance. The organization may also have to deal with compatibility, interoperability, or data quality issues when switching to a new application2. Option B, performing an analysis to determine the business risk, is a necessary step but not a recommendation for the organization. The organization should already be aware of the business risk of using an application whose vendor has gone out of business and whose escrow has an older version of the source code. The organization should focus on finding and implementing a solution to mitigate or eliminate this risk3. Option D, developing a maintenance plan to support the application using the existing code, is not a feasible option because it assumes that the organization has access to the existing code. However, this is not the case because the vendor has gone out of business and the escrow has an older version of the source code. The organization cannot support or maintain an application without having a complete and accurate copy of its source code.
References:
* How Important Is Source Code Escrow - ISACA1
* The What and Why of Source Code Escrow2
* Unlocking Source Code In Escrow 2023: A Guide To Secure Software3

NEW QUESTION: 95
□□□□ □□(□: □□□)□ □□ IP □□□ □□□ □ □□ □□ □□□ □□□□ □□ □ □□□ □□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□□ □□ □ □□□□□?
A. □□□ □□□□ □□□□
B. □□ □□ □□□□/□□□ □□□□(TCP/IP)
C. □□ □ □□□ □□□□
D. □□□ □□ □□□ □□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 96
□□ □ □□□□ □□□ □□□ □□ □□□ □ □□ □□□□ □□ □□□□□?
A. □□□ □□□□□ □□ □□ □□ □□ □□□
B. □□ □□ □ □□ □□□□ □□.
C. □□□ □□ □□ □□□ □□
D. □□ □□ □□□ □□ □□ □□ □ □□
Answer: C (LEAVE A REPLY)
Linking incidents to problem management activities would most effectively help to reduce the number of repeated incidents in an organization, because problem management aims to identify and eliminate the root causes of incidents and prevent their recurrence. Testing incident response plans, prioritizing incidents, and training incident management teams are all good practices, but they do not directly address the issue of repeated incidents.
References: ISACA ITAF 3rd Edition Section 3600

NEW QUESTION: 97
IS □□□□ □□□□□ □□□□□ □□□□□, □□ □□ □□□□ □□ □□□□□ □□ □□□□.
□□ □□□ □□□□ □□ □□ IS □□□□ □□□ □ □□ □□ □□□ □□ □ □□□□ □?
A. □□ □□□□□□□ □□□ □□□ □□ □□□ □□□□.
B. □□□□□ □□□□□□□ □□□ □□□ □□ □□□ □□□□.
C. □□ □ □□ □□□ □□□□□□□ □□□□ □□□□ □□ □□□ □□□□.
D. □□ □□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
□ □□□ □□ □□ □□ □□□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□□. □□□□ □□ □□□ □□ □□□ □□□ □, □□ □ □□ □□□ □ □ □□□ □□□□□?
A. □□□□□ □□□ □□□□ □□□□□ □□□□□.
B. □□ □□□□ □□□□ □□ □□(QA)□ □□□ □□□□ □□□□.
C. □□□□ □□ □□□ □□□□□ □□□□□.
D. □□ DevSecOps □□□□□ □□□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
Change control is the process of managing and documenting changes to an information system or its components. Change control aims to ensure that changes are authorized, tested, approved, implemented, and reviewed in a controlled and consistent manner. Change control is an essential part of ensuring the security, reliability, and quality of an information system.
One of the key elements of change control is testing and approval from quality assurance (QA). QA is the function that verifies that the changes meet the requirements and

specifications, comply with the standards and policies, and do not introduce any errors or vulnerabilities. QA testing and approval provide assurance that the changes are fit for purpose, function as expected, and do not compromise the security or performance of the system.
An organization that has recently moved to an agile model for deploying custom code to its in-house accounting software system should still follow change control procedures, including QA testing and approval.
Agile development methods emphasize flexibility, speed, and collaboration, but they do not eliminate the need for quality and security checks. In fact, agile methods can facilitate change control by enabling frequent and iterative testing and feedback throughout the development cycle.
However, if change control does not include testing and approval from QA, this poses a significant security concern for the organization. Without QA testing and approval, the changes may not be properly validated, verified, or evaluated before being deployed to production. This could result in introducing bugs, defects, or vulnerabilities that could affect the functionality, availability, integrity, or confidentiality of the accounting software system. For example, a change could cause data corruption, performance degradation, unauthorized access, or data leakage. These risks could have serious consequences for the organization's financial operations, compliance obligations, reputation, or legal liabilities.
Therefore, change control that does not include testing and approval from QA is the most significant security concern to address when reviewing the procedures in place for production code deployment in an agile model.
References:
* Change Control - ISACA
* Quality Assurance - ISACA
* Agile Development - ISACA
* 10 Agile Software Development Security Concerns You Need to Know

NEW QUESTION: 99
□□ □□ □□ □□(KPI) □□□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □ □□ □□□□□□□ □□□□ □□ □□□□□?
A. □□ □□□ □□□□ □□□□ □□□□ □□□□ □ □□□ □□
B. □□□ □□ □□□ □
C. □□ □□ □□□□ □□ □□□□□ □□
D. □□ □□ □□□□ □□ □
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Thespeed at which security threats are mitigatedis akey indicatorof an organization'srisk management effectiveness.

* Option A (Correct):Response time to security threatsmeasures how efficiently security teams detect, analyze, and mitigate risks, providingclear insight into security operations.
* Option B (Incorrect):The number of security controls auditeddoes not indicatehow well risk is being managed, only that reviews are taking place.
* Option C (Incorrect):Log analysis speedis useful, but it does notdirectly measure risk mitigation effectiveness.
* Option D (Incorrect):Risk register entriesindicate known risks but do not provide insight intohow well those risks are managed.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coverssecurity metrics, KPIs, and risk management evaluation.

NEW QUESTION: 100
□□□ □□ □□ □□□ □□ □□□□ □□ □□□□ □□□ □□ □□ □ □□□ □□ □ □□□ □□□ □□□ □ □□ □□ □□□□□?
A. □□□ □□ □□ □□ □□ □□□ □□□□ □□□□.
B. □□ □□□ □□ □□ □□ □□□□□ □□□□ □□□□.
C. □□ □□□ □□ □□ □□□□□ □□□□ □□□□□.
D. □□ □□□ □□ □□□ □□ □□ □□ □□□ □□□□ □□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
IS □□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□. □□□ □□□ □□□□ □□□ □ □□□□ □□ □□□□ □□□ □□ □□□ □ □ □□□ □□ □□□□ □□□□□ □□□?
A. □□ □□□
B. □□□ □□□
C. □□
D. □□□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 102
IS □□□□ □□□□□ □□□□ □□□ □□□ □□□□□ □□□ □□□□□. □□ □ □□ □□ □□□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□
B. □□□ □□□ □□
C. □□□□ □□ □ □□ □□ □□ □□
D. □□□ □□□ □ □□□□□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103

□□ □□ □□□ □□ □□ □□□ □□□□ □□ IS □□□□ □□□ □□□ □□□□ □ □ IT □□□ □□ □□□ □□□ □□□□□□. □□ □ □□□□ □□□ □□□ □□□□ □?

A. □□ □□ □□□□ □□□ □□□ □□□ □□□□□.

B. □□□ □□ □□□ □□□ □□□□ □□□□□.

C. □□ □□ □□□ □□□□□ □□ □□□ □□□ □□□.

D. □□ □ □□ □□ □□□ □□□ □□□ □□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 104

□□□ □□ □□□□ □□□□□□□ □□□□ □□□□□ □□□□ □□□□□□□□ □ □ □□□□ □□□□□. □□ □ IS □□□□ □□□ □□□□ □□□□ □□ □□□ □□ □□ □□□□□?

A. □□□ □□□ □□ □□□□ □□□ □ □□□□.

B. □□□ □□ □□□ □□□□ □□□ □□□□ □□□□.

C. □□□□ □□ □□□ □□□ □□ □□□□□.

D. □□□□ □□ □□ □□□□ □□□ □ □□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 105

□□ □ □□ □□□ □□□ □□□ □□ □□□□ □□ □□ □□□□?

A. □□ □□□□ □□□□ □□□ □□□ 90□ □ □□□□□.

B. □□□□□□ □□□ □□□□ □□□□ □□ 180□□□ □□□□□.

C. □□ □□□□ □□ □□□□ □□□□ □□□□ □□ □□ □□□□□ □□□□□.

D. □□□ □□ □□□□ □□ □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

This control is best implemented through system configuration because it can be enforced automatically by setting a parameter in the network operating system or directory service. This ensures that temporary workers do not have access to the network beyond their authorized period, and reduces the risk of unauthorized or malicious use of their accounts12.

References1: Configuration and Change Management - CISA2: What is IT Governance? - Definition from Techopedia

NEW QUESTION: 106

□□□□ □□□ □□□ □□ □□(DLP) □□□□□ □□□□□ □□□. □ □□ □□□ □ □□ □□□□ □□□□.

A. □□□ □□□

B. □□□ □□

C. □□ □□ □□

D. □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
□□ □□ □□□ □□□□□ □ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □□□□ □□ □□□ □□□□□ □□□ □ □□ □□□ □□ □ □□□□.
B. □□ □ □□□ □□□ □□□□□ □□ □□□ □□□□□□□.
C. □□ □□□□□ □□ □□□ □□ □□□□□ □□□□□.
D. □□ □□□□ □□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:Documenting anomalies in audit workpapers (D) is the best approach because it ensures traceability, supports findings in the audit report, and allows for future reference if similar issues arise. Even if an anomaly is low-risk, proper documentation is a fundamental audit practice.
Other options:
* Reprioritizing testing (A) is a valid audit approach but does not address documentation needs.
* Updating the audit plan (B) may be necessary but does not replace documentation.
* Prompt remediation (C) is an operational concern but is not always the auditor's primary role.
Reference: ISACA CISA Review Manual, Audit Process

NEW QUESTION: 108
□□ □□ IS □□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□, □□ □ □□□ □□□□□.
B. □□ □□ □□□ □□□□ □ □□□ □□□ □□□ □□□□
C. □□□ □□ □□ □□ □□ □□ □□□ □□□ □□□□ □□
D. □□ □□□ □□□□ □□ □□□□□ □□□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 109

□□□□□ □□□ □□□ □□□ □□ □□□ □□□□ □□□□ □□□□. □□□□□ □ □□ □□□ □□□□ □□ □□□□□□ □□□ □□□□. □□□□ □□□□ □□ □□□ □ □□□ □□□□ □ □□ □□□ □□ □□□ □□ □ □□ □□□□?

A. 24□□ □□□□□ □□□□ □□□ □□□□ □□□.

B. □□□□□ □□□□ □□ □□ □□(DRP)□ □□□ □□□ □□□.

C. □□□□□□ □□ □□□ □□□□□ □□□□□ □□□.

D. □□□□□ □□□ □□□□ □□□ □□□□□□ □□□□□ □□□□ □□□.

Answer: (SHOW ANSWER)

Source code for the software must be placed in escrow is the most important requirement to include in the vendor contract to ensure continuity. Source code is the original code of a software program that can be modified or enhanced by programmers. Placing source code in escrow means depositing it with a trusted third party who can release it to the customer under certain conditions, such as vendor bankruptcy, breach of contract, or failure to provide support. This can help to ensure continuity of the software product and its maintenance in case of vendor unavailability or dispute. The other options are less important requirements to include in the vendor contract, as they may involve support availability, disaster recovery plan, or staff training. References:

* CISA Review Manual (Digital Version), Chapter 5, Section 5.51
* CISA Review Questions, Answers & Explanations Database, Question ID 228

NEW QUESTION: 110

□□ □□□ □□□□□□□ □□□ □□□ □□□□ □□□□□ □□□□ □□ □□□ □ □□□□□. □□ □□□ □□□□ □□ □□ □□□ □□□ □□□□□?

A. □□ □□□ □□

B. □□ □□□ □□□□□.

C. □□ □□□ □□□□□.

D. □□ □□□□ □□□□□.

Answer: B (LEAVE A REPLY)

The most important action before the audit work begins is to establish control objectives. Control objectives are the specific goals or outcomes that the audit intends to achieve or verify in relation to the information protection in the application1. Control objectives provide the basis for designing and performing the audit procedures, evaluating the audit evidence, and reporting the audit findings and recommendations2. Control objectives also help to align the audit scope and criteria with the business needs and expectations, and to ensure that the audit is relevant, reliable, and efficient3.

Some examples of control objectives for an information protection audit are:

To ensure that the information stored in the application is classified according to its sensitivity, value, and regulatory requirements To ensure that the information stored in the application is encrypted, masked, or anonymized as appropriate To ensure that the information stored in the application is accessible only by authorized users and processes To ensure that the information stored in the application is backed up, restored, and

retained according to the business continuity and retention policies To ensure that the information stored in the application is monitored, logged, and audited for any unauthorized or anomalous activities Therefore, option B is the correct answer.
Option A is not correct because reviewing remediation reports is not the most important action before the audit work begins. Remediation reports are documents that describe how previous audit findings or issues have been resolved or addressed by the auditee4. While reviewing remediation reports may be useful for understanding the current state of information protection in the application, it is not a prerequisite for defining the control objectives of the audit.
Option C is not correct because assessing the threat landscape is not the most important action before the audit work begins. The threat landscape is the set of potential sources, methods, and impacts of cyberattacks or data breaches that may affect the information stored in the application5. While assessing the threat landscape may be helpful for identifying and prioritizing the risks and vulnerabilities of information protection in the application, it is not a prerequisite for defining the control objectives of the audit.
Option D is not correct because performing penetration testing is not the most important action before the audit work begins. Penetration testing is a technique that simulates real-world cyberattacks or data breaches to test the security and resilience of information systems or applications.

NEW QUESTION: 111
□□ □ IS □□□□ □□□□□ IT □□□□ □□□□□ □□□ □□□□ □□□□ □□ □ □ □□ □□□ □□□□□?
A. □□□□□□ □□ □□□□ □□ IT □□□□□ □□□□□□.
B. □□□□□□ □□□ □□□ □□ □□ □ □□□□ □ □□□□.
C. □□□□□□ □□ □□ □□(CSA)□ □□□□ □□ □ □□□ □□□.
D. □□□□□□ □□□ IT □□□ □□□□ □□□□ □ □□□ □□□.
Answer: B (LEAVE A REPLY)
The best reason for an IS auditor to emphasize to management the importance of using an IT governance framework is that frameworks can be tailored and optimized for different organizations. An IT governance framework is a set of principles, guidelines, and processes that help an organization align its IT strategy with its business goals, manage IT risks and performance, and deliver value from IT investments. An IT governance framework can be adapted and customized to suit the specific needs, context, and culture of each organization, taking into account factors such as size, industry, maturity, objectives, and stakeholders. An IT governance framework can also help an organization adopt best practices and standards from various sources, such as COBIT2, ITIL3, ISO/IEC 200004, and others.
The other options are not as good as option B, as they may not capture the full scope or benefits of using an IT governance framework. Frameworks enable IT benchmarks against competitors, but this is not the main purpose or advantage of using an IT governance

framework. Frameworks help facilitate control self- assessments (CSAs), but this is only one aspect or tool of an IT governance framework. Frameworks help organizations understand and manage IT risk, but this is also only one outcome or objective of an IT governance framework.
References:
* 1: What is ITIL? Your guide to the IT Infrastructure Library | CIO
* 2: IT Governance Framework | Components | Framework | Terminology - EDUCBA
* 3: IT Governance: Definitions, Frameworks and Planning - ProjectManager
* 4: What Is IT Governance? - Definition from Techopedia
* 5: What is IT Governance? A formal way to align IT & business strategy | CIO
* 6: What Is IT Governance? - Definition from WhatIs.com
* 7: ISO/IEC 20000 Information Technology Service Management Systems Standard - ISO/IEC 20000 Portal
* 8: COBIT | Control Objectives for Information Technologies | ISACA

NEW QUESTION: 112
IS □□□□ IT □□ □□ □□□ □□□□□ □□□ □ □□ □□□□ □□□ □□ □ □□ □□□□?
A. □□ □□□ □□□ □□□□ □□ □□ □□□□ □□□.
B. □□□□ □□□ □□□ □□ □□ □□□ □□□□□.
C. □□□□□ □□□□□ □□□□ □□□ □□□□□.
D. □□ □□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
□□ IT □□□□□□ □□□ □□□ □□ □□ □□□ □□□□ □, IS □□□□ □□ □□ □□□ □□ □ □□ □□ □□ □□□□ □□ □ □□ □□□?
A. □□□□ □□□ □□ □□ IT □□□□□□ □□□□□.
B. IT□ □□ □□ □□(KPI)□ □□□□□.
C. IT □□□□□□ □□ □□ □□□(ROI)□ □□□□□□.
D. □□□□ □□□ □□ □□ IT □□□□□□ □□□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 114
IS □□□□ □□□□ □□□□□□□□ □□ □□□ □□ □□□ □□□□□□ □□□ □ □□ □ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□
B. □□□□□□ □□ □□□
C. □□□ □□
D. □□ □□ □□
Answer: C (LEAVE A REPLY)

The type of review that is most important to conduct when an IS auditor is informed that a recent internal exploitation of a bug has been discovered in a business application is C. Forensic audit. A forensic audit is a type ofaudit that involves collecting, analyzing, and preserving evidence of fraud, corruption, or other illegal or unethical activities1. A forensic audit can help the IS auditor to identify and document the source, scope, and impact of the exploitation, as well as the perpetrators, motives, and methods involved. A forensic audit can also help the IS auditor to provide recommendations for preventing or mitigating future exploitations, and to support any legal actions or investigations that may arise from the incident2.

NEW QUESTION: 115
IS □□□□ □□ □□□□ □□□□ IT □□□ □□ □□□□□□ □□□ □□□□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□□□. □□ □ □□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □ □□□□ □□ □□□ □□ □□□ □□□ □ □□□□□ □ □□ □□□ □□□?
A. □□□□ □□
B. □□□ □□ □□
C. IT □□□□ □□□□□
D. □□□□□ □□
Answer: D (LEAVE A REPLY)
The most helpful tool in matching demand for projects and services with available resources in a way that supports business objectives is portfolio management. Portfolio management is the process of selecting, prioritizing, balancing and aligning IT projects and services with the strategic goals and value proposition of the organization3. Portfolio management helps the IT organization to allocate resources efficiently and effectively, to deliver value to the business units, and to align IT initiatives with business strategies. Project management, risk assessment results and IT governance framework are also important tools, but they are not as helpful as portfolio management in matching demand and supply of IT projects and services. References:
* CISA Review Manual, 27th Edition, page 721
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 116
IS □□□□ □□ □□□□□ □□□□ □□ □□ □□□□□ □□ □□□ □□ □□□ □ □□ □□ □□□□□□. □□□ □□ □□□ □□ □□ □ □□ □□□ □□ □ □□□□ □?
A. □□□□□ □□□□ □□□□ □□□ □□□ □ □□□□.
B. □□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □ □□□ □.
C. □□ □□□ □□ □□ □□ □□ □□□ □□□□ □□□□□.
D. □□□ □□ □□□ □□□□ □□□ □□□ □□□□.

Answer: (SHOW ANSWER)

The greatest concern with the lack of structure for technology risk governance is C. Key decision-making entities for technology risk have not been identified. Technology risk governance is the process of establishing and maintaining the policies, roles, responsibilities, and accountabilities for managing technology risks within an organization1. Technology risk governance requires a clear organizational structure that defines who has the authority and responsibility to make decisions, set objectives, allocate resources, monitor performance, and ensure compliance for technology risk management2. Without such a structure, an organization may face the following challenges:

Lack of alignment and integration between technology and business strategies, leading to suboptimal outcomes and missed opportunities.

Lack of clarity and consistency in technology risk identification, assessment, mitigation, and reporting, leading to gaps and overlaps in risk coverage and exposure.

Lack of communication and collaboration among different stakeholders involved in technology risk management, leading to conflicts and inefficiencies.

Lack of oversight and accountability for technology risk management activities and results, leading to poor quality and reliability.

NEW QUESTION: 117

□□□ □□□□ □□□ □ IS □□□□ □□□□ □ □□ □□□ □□□ □□□□□?

A. □□□ □□□ □□ □□□□□ □□□□□.

B. □□□ □□□□ □□ □□□ □□□□□.

C. □□□ □□□ □□□□ □□□□.

D. □□ □□□ □□ □□□□ □□□□ □□□□.

Answer: A (LEAVE A REPLY)

A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can help protect an organization's network and information systems from unauthorized or malicious access, by filtering or blocking unwanted or harmful packets. The most important thing for an IS auditor to verify when evaluating an organization's firewall is that the logs are being collected in a separate protected host. Logs are records of events or activities that occur on a system or network, such as connections, requests, responses, errors, and alerts. Logs can provide valuable information for auditing, monitoring, troubleshooting, and investigating security incidents. However, logs can also be tampered with, deleted, or corrupted by attackers or insiders who want to hide their tracks or evidence of their actions.

Therefore, it is essential that logs are stored in a separate host that is isolated and secured from the network and the firewall itself, to prevent unauthorized access or modification of the logs. Automated alerts are being sent when a risk is detected is a good practice for enhancing the security and efficiency of a firewall, but it is not the most important thing for an IS auditor to verify, as alerts may not always be accurate, timely, or actionable. Insider attacks are being controlled is a desirable outcome for a firewall, but it is not the most

important thing for an IS auditor to verify, as insider attacks may involve other factors or methods that bypass or compromise the firewall, such as social engineering, credential theft, or physical access. Access to configuration files is restricted is a critical control for ensuring the security and integrity of a firewall, but it is not the most important thing for an IS auditor to verify, as configuration files may not reflect the actual state or performance of the firewall.

NEW QUESTION: 118
IS □□□□ □□ □□□□ □□□ □□□□ □□□ □□(BCP)□ □□□ □□ □□ □□ (RPO)□ □□ □□□□ □□□□ □□ □□□□□□. □□□□ □□□ □□□ □□ □□ □?
A. □□ □□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□□□ □□□ □□□□□.
D. □□□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 119
□□□ □□□ □□ □□□□□ □□□ □ IS □□□□ □□ □□□ □□ □□□ □□□ □ □□.
A. □□□ □□□ □□□□□□.
B. □□□ □□□ □□□□□.
C. □□□ □□ □□ □□□ □□□□ □□□□ □□□□.
D. □□□□ □□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
Data classification is the process of organizing and labeling data into categories based on file type, contents, and other metadata. Data classification helps organizations answer important questions about their data that inform how they mitigate risk and manage data governance policies. Data classification also enables appropriate protection measures, and efficient search, retrieval and use of each data category12.
While evaluating the data classification process of an organization, an IS auditor's primary focus should be on whether data is correctly classified. This means that the data is assigned to the appropriate classification level based on its sensitivity, importance, integrity, availability, compliance requirements, and business value. Correct data classification ensures that the data is protected according to its risk level, and that the organization can comply with relevant laws and regulations that apply to different types of data3.
The other three options are not the primary focus of an IS auditor while evaluating the data classification process, although they may be relevant or useful for certain aspects of data management. Data classifications are automated means that the organization uses software tools or algorithms to analyze and label data based on predefined rules or criteria.

This can improve the efficiency and consistency of data classification, but it does not guarantee that the data is correctly classified. The IS auditor still needs to verify the accuracy and validity of the automated classifications, and check for any errors or anomalies.
A data dictionary is maintained means that the organization keeps a record of the definitions, formats, sources, and relationships of the data elements in its systems or databases. This can enhance the understanding and usability of the data, but it does not ensure that the data is correctly classified. The IS auditor still needs to examine the content and context of the data, and compare it with the classification criteria and policies.
Data retention requirements are clearly defined means that the organization specifies how long it will keep different types of data, and when it will delete or archive them. This can help reduce storage costs, improve performance, and comply with legal obligations, but it does not ensure that the data is correctly classified. The IS auditor still needs to assess whether the data is stored and protected according to its classification level, and whether the retention periods are appropriate for each type of data.
Therefore, data is correctly classified is the best answer.
References:
* Data Classification: The Basics and a 6-Step Checklist - NetApp
* What is Data Classification? Guidelines and Process -Varonis
* Data Classification and Handling Procedures Guide

NEW QUESTION: 120
□□ □ □□□ □□□ □□□□ □ □□□ □□ □□ □□□□ □□ □□ □□□□ □□□ □ □□ □□ □□□ □□□□□?
A. □□□
B. □□
C. □□ □□
D. □□□ □□
Answer: D (LEAVE A REPLY)
The best way to sanitize a hard disk for reuse to ensure the organization's information cannot be accessed is data wiping. Data wiping is a process that overwrites the data on the hard disk with random or meaningless patterns, making it unrecoverable by any software or hardware methods. Data wiping can provide a high level of security and assurance that the organization's information is permanently erased from the hard disk, and that it cannot be accessed by unauthorized parties or malicious actors.
Re-partitioning is not a way to sanitize a hard disk for reuse, but rather a way to organize the hard disk into different logical sections or volumes. Re-partitioning does not erase the data on the hard disk, but only changes the structure and allocation of the disk space. Re-partitioning may make the data inaccessible to the operating system, but not to other tools or methods that can scan or recover the data from the disk sectors.

Degaussing is a way to sanitize a hard disk for reuse, but only for magnetic hard disks, not solid state drives (SSDs). Degaussing is a process that exposes the hard disk to a strong magnetic field, which disrupts and destroys the magnetic alignment of the data on the disk platters. Degaussing can effectively erase the data on magnetic hard disks, but it can also damage or render unusable the electronic components of the hard disk, such as the read/write heads or circuit boards. Degaussing also does not work on SSDs, which store data using flash memory cells, not magnetic media.
Formatting is not a way to sanitize a hard disk for reuse, but rather a way to prepare the hard disk for use by an operating system. Formatting is a process that creates a file system on the hard disk, which defines how the data is stored and accessed on the disk. Formatting does not erase the data on the hard disk, but only deletes the file system metadata and marks the disk space as available for new data. Formatting may make the data invisible to the operating system, but not to other tools or methods that can restore or recover the data from the disk sectors.
References:
* How to Wipe A Hard Drive for Reuse? Check the Quickest Way to Wipe A Hard Drive - EaseUS 1
* HP PCs - Using Secure Erase or HP Disk Sanitizer 2
* HOW to QUICKLY and PERMANENTLY SANITIZE ANY DRIVE (SSD, USB thumb drive ...)

NEW QUESTION: 121
□□□ □□□ □□ □□□ □□□□□ □□□ □ IS □□□□ □□ □ □□ □□□ □□□ □ □□□?
A. □□□ □□□ □□□ □□ □□ □□□□
B. □□ □□ □□□□ □□□ □□□□ □□□□ □□
C. □□ □□□□ □□□□□ □□ □□ □□□□
D. □□ □□□ □□□ □□□ □□ □□
Answer: A (LEAVE A REPLY)
Information systems governance is the set of policies, processes, structures, and practices that ensure the alignment of IT with business objectives, the delivery of value from IT investments, the management of IT risks, and the optimization of IT resources1.
Information systems governance is a strategic and high-level function that covers the entire organization and its IT portfolio. Therefore, an IS auditor should review the aspects of information systems governance that are relevant to the organization's vision, mission, goals, and strategies.
One of the aspects that an IS auditor should review when evaluating information systems governance for a large organization is the approval processes for new system implementations. This is because new system implementations are significant IT investments that require careful planning, analysis, design, development, testing, deployment, and evaluation to ensure that they meet the business requirements, deliver

the expected benefits, comply with the relevant standards and regulations, and minimize the potential risks2. The approval processes for new system implementations should involve the appropriate stakeholders, such as senior management, business owners, IT managers, project managers, users, and auditors, who have the authority and responsibility to approve or reject the proposed system implementations based on predefined criteria and metrics3. The approval processes for new system implementations should also be documented, transparent, consistent, and timely to ensure accountability and traceability4. Therefore, an IS auditor should review the approval processes for new system implementations to assess whether they are aligned with the information systems governance framework and objectives.
The other possible options are:
* Procedures for adding a new user to the invoice processing system: This is an operational task that involves granting access rights and permissions to a specific user for a specific system based on the principle of least privilege. This is not a strategic or high-level function that falls under information systems governance. Therefore, an IS auditor should not review this aspect when evaluating information systems governance for a large organization.
* Approval processes for updating the corporate website: This is a tactical task that involves making changes or enhancements to the content or design of the corporate website based on the business needs and feedback. This is not a strategic or high-level function that falls under information systems governance. Therefore, an IS auditor should not review this aspect when evaluating information systems governance for a large organization.
* Procedures for regression testing system changes: This is a technical task that involves verifying that existing system functionalities are not adversely affected by new system changes or updates. This is not a strategic or high-level function that falls under information systems governance. Therefore, an IS auditor should not review this aspect when evaluating information systems governance for a large organization. References: 1: What is IT Governance? - Definition from Techopedia 2: System Implementation - an overview | ScienceDirect Topics 3: Project Approval Process - Project Management Knowledge 4: 5 Best Practices For A Successful Project Approval Process | Kissflow Project : Principle of Least Privilege (POLP) | Imperva : How to Update Your Website Content - 7 Step Guide | HostGator Blog : What Is Regression Testing? Definition & Best Practices | BrowserStack

NEW QUESTION: 122
□□□ □□□ □□ □□ □□□□ □□□□□ □□□□ □□ □□□ □ □□ □□ □ □□ □ □□□□□?
A. □□□□ □□□□ □ □□□□ □□
B. □□□□ □□□□□ □□ □□ □□
C. □□□□ □□ □□□□ □□ □□
D. □□ □ □□ □□□□ □□□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
□□ □ RSA □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□ □□ □□□□ □ □□□ □□ □□ □□□□□?
A. □□□□□□ □□□□ □□ □□ □□
B. □□ □□□ □□□ □□
C. □□□□ □□□ □□□□
D. □□□□ □□□ □□
Answer: (SHOW ANSWER)
A digital signature is a cryptographic technique that verifies the authenticity and integrity of a message or document, by using a hash function and an asymmetric encryption algorithm. A hash function is a mathematical function that transforms any input data into a fixed-length output value called a digest, which is unique for each input. An asymmetric encryption algorithm uses two keys: a public key and a private key.
The public key can be shared with anyone, while the private key must be kept secret by the owner. To create a digital signature, the sender first applies a hash function to the plaintext message to generate a digest. Then, the sender encrypts the digest with their private key to produce the digital signature. To verify the digital signature, the receiver decrypts the digital signature with the sender's public key to obtain the digest. Then, the receiver applies the same hash function to the plaintext message to generate another digest. If the two digests match, it means that the message has not been altered and that it came from the sender. The security of a digital signature depends on the secrecy of the sender's private key. If an attacker obtains the sender's private key, they can create fake digital signatures for any message they want, thus compromising the control provided by the digital signature. Reversing the hash function using the digest is not possible, as hash functions are designed to be one-way functions that cannot be inverted. Altering the plaintext message will result in a different digest after applying the hash function, which will not match with the decrypted digest from the digital signature, thus invalidating the digital signature. Deciphering the receiver's public key is not relevant, as public keys are meant to be publicly available and do not affect the security of digital signatures.

NEW QUESTION: 124
□□ □□ □□ □□ □□ □□□ □□ □□□□ □□ □□ □□ □□□□□?
A. □□ □□
B. □□ □□□
C. □□ □□
D. □□ □□□
Answer: (SHOW ANSWER)
Among the options provided, fingerprint scanning has the highest rate of false negatives. False negatives occur when a biometric system fails to recognize an authentic individual. Factors such as skin conditions (wet, dry, greasy), finger injuries, and inadequate scanning can contribute to false negatives in fingerprint scanning1. In comparison, iris recognition23, face recognition45, and retina scanning67 generally have lower rates of false negatives.
References:
How Accurate are today's Fingerprint Scanners? - Bayometric
25 Advantages and Disadvantages of Iris Recognition - Biometric Today
Iris Recognition Technology (or, Musings While Going through Airport ...
The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist | ITIF NIST Launches Studies into Masks' Effect on Face Recognition Software Retinal scan - Wikipedia How accurate are retinal security scans - Smart Eye Technology

NEW QUESTION: 125
□□ □ □□□ □□□□ □□ □□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□□ □□
B. □□ □□□ □□
C. □□ □ □□
D. □□ □□ □□(BIA)
Answer: C (LEAVE A REPLY)
This is the most helpful method for measuring benefits realization for a new system, because it involves evaluating the actual outcomes and impacts of the system after it has been implemented and used for a certain period of time. A post-implementation review can compare the actual benefits with the expected benefits that were defined in the business case or the benefits realization plan, and identify any gaps, issues, or opportunities for improvement. A post-implementation review can also assess the effectiveness, efficiency, and satisfaction of the system's users, stakeholders, and customers, and provide feedback and recommendations for future enhancements or changes.
The other options are not as helpful as post-implementation review for measuring benefits realization for a new system:
* Function point analysis. This is a technique that measures the size and complexity of a software system based on the number and types of functions it provides. Function point

analysis can help estimate the cost, effort, and time required to develop, maintain, or enhance a software system, but it does not measure the actual benefits or value that the system delivers to the organization or its users.
* Balanced scorecard review. This is a strategic management tool that measures the performance of an organization or a business unit based on four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard review can help align the organization's vision, mission, and goals with its activities and outcomes, but it does not measure the specific benefits or impacts of a new system.
* Business impact analysis (BIA). This is a process that identifies and evaluates the potential effects of a disruption or disaster on the organization's critical business functions and processes. A BIA can help determine the recovery priorities, objectives, and strategies for the organization in case of an emergency, but it does not measure the benefits or value of a new system.

NEW QUESTION: 126
□□ □□□ □□□□ IT □□□□ □□□□ □□ □□□ □□□ □□□□ □□ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□ □□□□□ □□□ □□□ □□□.
B. □□ □□ □□□ □□□□□ □□□□□.
C. □□□ □□ □□□ □□ □□□□ □□□□□ □□□□□.
D. □□□ □□ □□□ □□ □□□□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The best control for detecting unauthorized data changes in an IT organization where many responsibilities are shared is to have data changes independently reviewed by another group. This is because an independent review can provide an objective and unbiased verification of the data changes and ensure that they are authorized, accurate, and complete. An independent review can also help to detect any errors, fraud, or malicious activities that may have occurred during the data changes. An independent review can also provide assurance that the data integrity and security are maintained.
References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.31
* CISA Online Review Course, Domain 1, Module 4, Lesson 22

NEW QUESTION: 127
IS □□□□ □□ □□□ □□□□ □□ □□ □□ □ □□ □□□ □□□□ □□□□ □□ □□ □□□□□?
A. □□ □□□ □□ □ 2□ □□ □□□□□.
B. □□ □□□ □□ □□□□□ □□□□.
C. □□ □□□□ □□ □□□ □□□□ □□□□□.
D. □□ □□□ □□□□ □ □□□□ □□□□□□ □□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
IS □□□□ □□□ □□□ □□□ □ □□ □ □□ □□ □□□□ □ □□□ □□□□□?
A. □□□ □□ □□
B. □□ □□□ □
C. □□□□ □□ □□
D. □□□□ □□□ □□
Answer: A (LEAVE A REPLY)
This should be the first thing that an IS auditor considers when evaluating firewall rules, because it defines the objectives, standards, and guidelines for securing the organization's network and information assets. The firewall rules should be aligned with the organization's security policy, and reflect the level of risk and protection required for each type of network traffic, system, or data. The IS auditor should compare the firewall rules with the security policy, and identify any discrepancies, gaps, or conflicts that could compromise the security or performance of the network.
The other options are not as important as the organization's security policy when evaluating firewall rules:
* The number of remote nodes. This is a factor that may affect the complexity and scalability of the firewall rules, but it is not a primary consideration for the IS auditor. Remote nodes are devices or systems that connect to the network from outside locations, such as teleworkers, mobile users, or branch offices. The IS auditor should ensure that the firewall rules provide adequate security and access control for remote nodes, but this depends on the organization's security policy and business needs.
* The firewalls' default settings. These are the predefined configurations that come with the firewall devices or software, and that determine how they handle network traffic by default. The IS auditor should review the firewalls' default settings, and verify that they are appropriate and secure for the organization's network environment. However, the firewalls' default settings may not match the organization's security policy or specific requirements, and may need to be customized or overridden by firewall rules.
* The physical location of the firewalls. This is a factor that may affect the placement and design of the firewall rules, but it is not a critical consideration for the IS auditor. The physical location of the firewalls refers to where they are installed or deployed in relation to the network topology, such as at the network perimeter, between network segments, or on individual hosts. The IS auditor should ensure that the firewall rules are consistent and coordinated across different locations, but this depends on the organization's security policy and network architecture.

NEW QUESTION: 129
CFO□ □□ □□ □□ □ □□□ □□ □□□ □□ □□□ □□ IT □□ □□□ □□ □□□ □□□□□□. □ □□□ □□□□□ □□□□ □□ □□ □□□□ □□□□ □ □□□ □ □□□□?

A. □□□ □□□□ □□ □□ □□□ □ □□ □□□□□ □□
B. □□□ □□□ □□□ □□□ □□□ □□□□□ □□
C. □□ □□□□ □□ □□□ □□□□ □□□ □□
D. □□ □□□□ □□□ □□□□ □ □□□ □□□ □□□ □□□ □□
Answer: (SHOW ANSWER)
The most important thing to consider before including an audit of IT capacity management in the program is whether the system's performance poses a significant risk to the organization. IT capacity management is a process that ensures that IT resources are sufficient to meet current and future business needs, and that they are optimized for cost and performance. A poor IT capacity management can result in system slowdowns, outages, failures, or breaches, which can affect the availability, reliability, security, and efficiency of IT services and business processes. Therefore, before conducting an audit of IT capacity management, the auditor should assess the potential impact and likelihood of these risks on the organization's objectives, reputation, compliance, and customer satisfaction.
Whether system delays result in more frequent use of manual processing (option A) is not the most important thing to consider before including an audit of IT capacity management in the program, as it is only one possible consequence of poor IT capacity management. Manual processing can introduce errors, delays, inefficiencies, and inconsistencies in the data and reports, which can affect the quality and accuracy of financial information. However, manual processing is not the only or the worst outcome of poor IT capacity management; there may be other more severe or frequent risks that need to be considered.
Whether stakeholders are committed to assisting with the audit (option C) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the feasibility and effectiveness of the audit, not the necessity or priority of it. Stakeholder commitment is important for ensuring that the auditor has access to relevant information, documents, data, and personnel, as well as for facilitating communication, collaboration, and feedback during the audit process. However, stakeholder commitment is not a sufficient reason to conduct an audit of IT capacity management; there must be a clear risk-based rationale for selecting this area for audit.
Whether internal auditors have the required skills to perform the audit (option D) is also not the most important thing to consider before including an audit of IT capacity management in the program, as it is a factor that affects the quality and credibility of the audit, not the urgency or importance of it. Internal auditors should have the appropriate knowledge, skills, and experience to perform an audit of IT capacity management, which may include technical, business, analytical, and communication skills. However, internal auditors can also acquire or supplement these skills through training, coaching, consulting, or outsourcing.
Therefore, internal auditors' skills are not a decisive factor for choosing this area for audit.
Therefore, option B is the correct answer.

References:
* Guide to IT Capacity Management | Smartsheet
* ISO 27001 capacity management: How to implement control A.12.1.3 - Advisera
* ISO 27002:2022 - Control 8.6 - Capacity Management

NEW QUESTION: 130
IS □□□□ □□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□□ □□ □ □□ □□ □□ □□□ □□□□□□. □□□□ □□ □□□ □□ □ □□ □□□□?
A. □□□ □□□ □□□□□.
B. □□ □□ □□□□□ □□□□□.
C. □□ □□ □□□□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The change management process is the set of procedures and activities that ensure that changes to the information system are authorized, tested, documented, and implemented in a controlled manner12. A defect in a recent release indicates that there may be issues with the quality assurance, testing, or approval of the changes, which could affect the reliability, security, and performance of the system3 . Therefore, the auditor's next step should be to evaluate the change management process and identify the root cause of the defect, as well as the impact and remediation of the incident.
References
1: Change Management - CISA
2: What is Change Management? - Definition from Techopedia
3: How to Audit Change Management - ISACA Journal
The Business Case for Security | CISA

NEW QUESTION: 131
□□□□ □□ □□□□ □□ □□□ □□□ □□□□.
A. □□ □□ □□□ □□□□□.
B. □ □□□□ □□□□ □□□□□ □□□□□.
C. □□□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□.
D. □□□□□ □□□□□ □□□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The primary responsibility of a project steering committee is to provide regular project updates and oversight.
A project steering committee is an advisory group that consists of senior stakeholders and experts who offer guidance and support to a project manager and their team. The steering committee is mainly concerned with the direction, scope, budget, timeline, and methods used to realize a given project1.
One of the key roles of a steering committee is to monitor the progress and performance of the project and ensure that it aligns with the business objectives and stakeholder

expectations. The steering committee also provides feedback, advice, and recommendations to the project manager and helps them resolve any issues or challenges that may arise during the project lifecycle. The steering committee communicates regularly with the project manager and other stakeholders through meetings, reports, and presentations23.

Therefore, providing regular project updates and oversight is the primary responsibility of a project steering committee.

References:

Steering Committee: Definition, Roles & Meeting Tips - ProjectManager

Project Steering Committee: Roles, Best Practices, Challenges - ProjectPractical Steering Committee: Complete Guide with Examples & Templates - Status.net

NEW QUESTION: 132

□□ □ □□ □□□ □□ □□ □□□ □□□(EUC) □□□□□□□ □□□ □□ □ □□□ □□□□ □□ □□□□□?

A. □□□□ □□□□ □□□□ □□□ □ □□

B. □□□□ □□□ □□

C. □□ □□□□□ □□ □□ □□

D. □□□□□□□ □□ □□

Answer: (SHOW ANSWER)

Spreadsheets, often used in EUC, are prone to manual input errors and formula mistakes. These errors can significantly compromise the accuracy and integrity of financial reporting.

References

ISACA CISA Review Manual (Current Edition) - Chapter on End-User Computing (EUC) risks Industry Research on Spreadsheet Errors: Multiple studies highlight the prevalence of errors in spreadsheets, especially those used for financial purposes.

NEW QUESTION: 133

□□ □□ □□□□ IP □□ □□ □□□□ □□ □□□□□□□ □□□ □□□ □□□□□ □□. □ □□□ □□□ □□ □ □□□ □□□□□?

A. □□ □□□□□□□ □□□□ □□□ □□(BCF)□ □□□□ □□□□.

B. □□ □□□□□□□ □□□□ □□□□□ □□□□ □□ □ □□□□.

C. □□□□□□ □□□ □□ □□□ □□□ □□□□□.

D. □□□□ □□ □□ □□ □□□ □ □□□□.

Answer: B (LEAVE A REPLY)

The greatest risk associated with the situation of business units purchasing cloud-based applications without IT support is that the applications may not reasonably protect data. Cloud-based applications are software applications that run on the internet, rather than on a local device or network. Cloud-based applications offer many benefits, such as scalability, accessibility, and cost-effectiveness, but they also pose many challenges and risks, especially for data security1.

Data security is the process of protecting data from unauthorized access, use, modification, disclosure, or destruction. Data security is essential for ensuring the confidentiality, integrity, and availability of data, as well as complying with legal and regulatory requirements. Data security is especially important for cloud- based applications, as data are stored and processed on remote servers that are owned and managed by third- party cloud service providers (CSPs)2.
When business units purchase cloud-based applications without IT support, they may not be aware of or follow the best practices and standards for data security in the cloud. They may not perform adequate risk assessments, vendor evaluations, contract reviews, or audits to ensure that the CSPs and the applications meet the organization's data security policies and expectations. They may not implement appropriate data encryption, backup, recovery, or disposal methods to protect the data in transit and at rest. They may not monitor or control the access and usage of the data by internal or external users. They may not report or respond to any data breaches or incidents that may occur3.
These actions or inactions may expose the organization's data to various threats and vulnerabilities in the cloud, such as cyberattacks, human errors, malicious insiders, misconfigurations, or legal disputes. These threats and vulnerabilities may result in data loss, leakage, corruption, or compromise, which may have serious consequences for the organization's reputation, operations, performance, compliance, and liability4.
Therefore, it is essential that business units consult and collaborate with IT support before purchasing any cloud-based applications, and follow the organization's guidelines and procedures for cloud security. IT support can help business units to select and use cloud-based applications that are suitable and secure for their needs and objectives.
References:
* Top 5 Risks With Cloud Software and How to Mitigate Them4
* Mitigate risks and secure your cloud-native applications3
* 12 Risks, Threats & Vulnerabilities in Moving to the Cloud2
* Best Practices to Manage Risks in the Cloud1

NEW QUESTION: 134
□□ □□□□ □□ □□□ □□□□ □□ □□(RAID)□ □□□□ □□□□ □□□□ IS □ □□□ □□□□□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□□ □□□ □□□□□□ □□□ □ □□□□.
B. □□□ □□□□ □□ □□□ □□ □□□□ □ □□□□.
C. □□□ □□□ □□□□□ □□ □□□□.
D. □□□ □□ □□□□□ □□□ □ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 135
□□ □ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □□(DRP) □□

B. □□□□ □□ □□□□□
C. □□ □□
D. □□ □□□ □□ □□□□ □□ □□
Answer: B (LEAVE A REPLY)
Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom for its decryption1. Ransomware attacks can cause significant damage to an organization's operations, reputation, and finances1. Therefore, it is important to mitigate the impact of ransomware attacks by implementing effective prevention and recovery strategies.
One of the best ways to mitigate the impact of ransomware attacks is to back up data frequently12345. Data backups are copies of the organization's data that are stored in a separate location or medium, such as an external hard drive, cloud storage, or tape2. Data backups can help the organization restore its data in case of a ransomware attack, without paying the ransom or losing valuable information2. Data backups should be performed regularly, preferably daily or weekly, depending on the criticality and volume of the data2. Data backups should also be tested periodically to ensure their integrity and usability2.
The other options are not as effective as backing up data frequently in mitigating the impact of ransomware attacks. Invoking the disaster recovery plan (DRP) is a reactive measure that can help the organization resume its operations after a ransomware attack, but it does not prevent or reduce the damage caused by the attack3.
Paying the ransom is not a recommended option, as it does not guarantee the decryption of the data or the deletion of the stolen data by the attackers. Paying the ransom also encourages further attacks and funds criminal activities14. Requiring password changes for administrative accounts is a good security practice, but it is not sufficient to prevent or recover from ransomware attacks. Ransomware attacks can exploit other vulnerabilities, such as phishing emails, outdated software, or weak network security15.
References: 1: How to Mitigate the Risk of Ransomware Attacks: The Definitive Guide 2: Mitigating malware and ransomware attacks - The National Cyber Security Centre 3: 3 steps to prevent and recover from ransomware 4: Ransomware Epidemic: Use these 8 Strategies to Mitigate Risk 5: Practical Steps to Mitigate Ransomware Attacks - ITSecurityWire

NEW QUESTION: 136
□□ □ □□□ □□□□ □□□□□□□ □□□□ □ □□□ □□□□ □□□□ □ □□□ □ □□ □□ □□□□ □□□□□?
A. □□ □□□ □□
B. □□ □□ □□
C. □□ □□ □□□
D. □□□□□ □□ □□
Answer: (SHOW ANSWER)

Function point analysis (FPA) is the best methodology to use for estimating the complexity of developing a large business application. FPA is a technique that measures the functionality of a software system based on the user requirements and the business processes that the system supports. FPA assigns a numerical value to each function or feature of the system, based on its type, complexity, and relative size. The total number of function points represents the size and complexity of the system, which can be used to estimate the development effort, cost, and time.
FPA has several advantages over other estimation methods, such as:
* It is independent of the technology, programming language, or development methodology used for the system. Therefore, it can be applied consistently across different platforms and environments.
* It is based on the user perspective and the business value of the system, rather than the technical details or implementation aspects. Therefore, it can be performed early in the project life cycle, before the design or coding phases.
* It is objective and standardized, as it follows a set of rules and guidelines defined by the International Function Point Users Group (IFPUG). Therefore, it can reduce ambiguity and improve accuracy and reliability of the estimates.
* It is adaptable and scalable, as it can handle changes in the user requirements or the system scope.
Therefore, it can support agile and iterative development approaches.
References:
* 1: Function Point Analysis - Introduction and Fundamentals
* 2: Software Engineering | Functional Point (FP) Analysis

NEW QUESTION: 137
IS □□□□ □□□ □□□ □□ □ □□□□□□□ □□ □□□ □□ □□□ □□□□□ □□□□□ □□ □□□□□□. □□ □□□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□ □□□.
A. □□□□ □□ □□(SQL) □□
B. □□ □□□□.
C. □□□ □□(DoS).
D. □□.
Answer: A (LEAVE A REPLY)

Validation controls are used to check the input data from the user before processing it on the server. If the validation controls are moved from the server side to the browser, it means that the user can modify or bypass them using tools such as browser developer tools, JavaScript console, or proxy tools. This would increase the risk of a successful attack by structured query language (SQL) injection, which is a technique that exploits a security vulnerability in an application's software layer that allows an attacker to execute arbitrary SQL commands on the underlying database. SQL injection can result in data theft, data corruption, or unauthorized access to the system.
Buffer overflow, denial of service (DoS), and phishing are not directly related to the validation controls in a web application. Buffer overflow is a type of attack that exploits a memory management flaw in an application or system that allows an attacker to write data beyond the allocated buffer size and overwrite adjacent memory locations. DoS is a type of attack that prevents legitimate users from accessing a service or resource by overwhelming it with requests or traffic. Phishing is a type of attack that uses fraudulent emails or websites to trick users into revealing sensitive information or installing malware.
References:
Client-side form validation - Learn web development | MDN
JavaScript: client-side vs. server-side validation - Stack Overflow
SQL Injection - OWASP

NEW QUESTION: 138
IS □□□□ IT □□□□ □□□ □□□□ □□□ □□ □□□□□□ □□□ □□□□ □□ □□ □□ □□ □□□□□□ □□□□ □□□ □□ □□□□□□. □□ □□ □□ □ □□ □□ IT □□ □□□□ □□□□ □ □□ □ □□□ □□□□?
A. IT □□□□□ □□□□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□.
B. IT □□□□□ □□□ □□□□ □□ □□□ IT □□□□□□ □□□□.
C. □□□□ □□ □□□□ □□ IT □□□ □□□□□ □□□□□.
D. □□□□ □□□ □□ □□□□ □□□ □□ □□ □□ □□ IT □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
An IT steering committee is a group of senior executives and stakeholders who provide strategic direction, guidance, and oversight for the IT function of an organization. An IT steering committee can help to improve the maturity of the IT team by ensuring that the IT initiatives are aligned with the business goals and objectives, that the IT resources are allocated and utilized effectively and efficiently, and that the IT performance and value are measuredand communicated. An IT steering committee can also help to resolve conflicts, prioritize demands, and foster collaboration among the IT project managers and other business units.
References
ISACA CISA Review Manual, 27th Edition, page 254
Auditing IT Governance
The Impact of Poor IT Audit Planning and Mitigating Audit Risk

IS Audit Basics: The Components of the IT Audit Report

NEW QUESTION: 139
□□ □ □□□ □□ □□ □□□□□□ IS □□□□ □□ □□□ □□□□□?
A. □□□ □□ □□□□□ □□
B. □□□ □□□ □□□ □□ □□□□□ □□
C. □□ □□□ □□ □□□ □□□□□ □□
D. □□ □ □□ □□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
Validating that assets are protected according to assigned classification is the primary role of the IS auditor in an organization's information classification process. An IS auditor should evaluate whether the information security controls are adequate and effective in safeguarding the information assets based on their classification levels. The other options are not the primary role of the IS auditor, but rather the responsibilities of the information owners, custodians, or security managers. References:
* CISA Review Manual (Digital Version), Chapter 6, Section 6.2.31
* CISA Review Questions, Answers & Explanations Database, Question ID 206

NEW QUESTION: 140
□□ □□□ □□□□ □□□ □□□ □□□□ □□ □ □□ □□□ □□ □ □□□□□?
A. □□ □□□ □□
B. □□□ □□ □□
C. □□□ □□ □□
D. □□□□ □□ □□
Answer: (SHOW ANSWER)
The first step in managing the impact of a recently discovered zero-day attack is to identify vulnerable assets.
A zero-day attack is a cyberattack that exploits a previously unknown or unpatched vulnerability in a software or system, before the vendor or developer has had time to fix it. Identifying vulnerable assets is crucial for managing the impact of a zero-day attack, because it helps to determine the scope and severity of the attack, prioritize the protection and mitigation measures, and isolate or quarantine the affected assets from further damage or compromise. The other options are not the first steps in managing the impact of a zero-day attack, because they either require more informationabout the vulnerable assets, or they are part of the subsequentsteps of assessing, responding, or recovering from the attack. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 141
□□ □□□ □□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□□□ □□□, □□ □ □□□□, □□ □□□ □□(DDoS) □□□ □□□ □ □□□□?

A. □□□□ □□
B. □□ □□
C. □□□ □□□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 142
IT □□□□□ □□□□ □□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □ □□□□?
A. □□□□ □□ □□ □ □□□ □□
B. □□ □□□ □□ □□
C. □□□□ □ □□
D. □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 143
□□□ □□ □□□ □□□□□□□ □□□□ □□□ □□□ □□□□□□ □□□ □□□ □□□ □□□ □□□□□. □□ □ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□?
A. □□□ □□ □□□ □□□□ □□ □□□ □□□□.
B. □□□ □□ □□□□□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □□ □□□□ □□□□□.
D. □□□ □□□□ □□□□ □□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The best way to prevent accepting bad data from a third-party service provider is to implement business rules to reject invalid data. Business rules are logical statements that define the data quality requirements and standards for the organization. By implementing business rules, the organization can ensure that only data that meets the predefined criteria is accepted into the enterprise data warehouse. Obtaining error codes indicating failed data feeds, purchasing data cleansing tools from a reputable vendor, and appointing data quality champions across the organization are useful measures to improve data quality, but they do not prevent accepting bad data in the first place. References: ISACA Journal Article: Data Quality Management

NEW QUESTION: 144
IT □□□□ □□, □□ □ □□□ □□□ □□□□ □□ □ □□□□□.
A. □□□ □□ □□
B. □□ □□ □□(CSA).
C. □□□ □□ □□(SLA).
D. □□ □□□.
Answer: C (LEAVE A REPLY)

A service level agreement (SLA) is a contract between a service provider and a customer that defines the expected level of performance, risks, and capabilities of an IT infrastructure. An IS auditor can use an SLA to measure how well the IT infrastructure meets the business needs and objectives, as well as to identify any gaps or issues that need to be addressed. The other options are not directly related to measuring the performance, risks, and capabilities of an IT infrastructure. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.2.11
* CISA Review Questions, Answers & Explanations Database, Question ID 203

NEW QUESTION: 145
□□ □□□ □□□ □□□ □□ □□□□□ □□□ □□□□ □□ IP □□□ □□ □ □□ □□□ □□ IP □□□ □□□□□?
A. □□□
B. □□□□□□□(IPS)
C. □□□□□
D. □□□
Answer: D (LEAVE A REPLY)
A router is a type of device that sits on the perimeter of a corporate or home network, where it obtains a public IP address and then generates private IP addresses internally. A router connects two or more networks and forwards packets between them based on routing rules. A router can also provide network address translation (NAT) functionality, which allows multiple devices to share a single public IP address and access the internet. A switch is a type of device that connects multiple devices within a network and forwards packets based on MAC addresses. An intrusion prevention system (IPS) is a type of device that monitors network traffic and blocks or modifies malicious packets based on predefined rules. A gateway is a type of device that acts as an interface between different networks or protocols, such as a modem or a firewall. References: CISA Review Manual (Digital Version), [ISACA Glossary of Terms]

NEW QUESTION: 146
□□ □ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □ □□□□ □ □□□□?
A. □□ □□ □□ □□□
B. □□ □□□
C. □□ □□□ □□
D. □□□□ □□ □□□
Answer: C (LEAVE A REPLY)
Capability maturity models (CMMs) are frameworks that help organizations assess and improve their processes in various domains, such as software development, project management, service delivery, and cybersecurity1. CMMs define different levels of process maturity, from initial to optimized, and describe the characteristics and best practices of each level. By using CMMs, organizations can benchmark their current

processes against a common standard, identify gaps and weaknesses, and implement improvement actions to achieve higher levels of process maturity2. CMMs can also help organizations align their processes with their strategic goals, measure their performance, and increase their efficiency, quality, and customer satisfaction3.
Therefore, the use of CMMs would best enhance a process improvement program, as they provide a systematic and structured approach to evaluate and improve processes based on proven principles and practices. Option C is the correct answer.
Option A is not correct because model-based design notations are graphical or textual languages that help designers specify, visualize, and document the structure and behavior of systems4. While they can be useful for designing and communicating complex systems, they do not directly address the process improvement aspect of a program.
Option B is not correct because balanced scorecard is a strategic management tool that helps organizations translate their vision and mission into measurable objectives and indicators. While it can be useful for monitoring and evaluating the performance of a program, it does not provide specific guidance on how to improve processes.
Option D is not correct because project management methodologies are sets of principles and practices that help organizations plan, execute, and control projects. While they can be useful for managing the scope, schedule, cost, quality, and risk of a program, they do not focus on the process improvement aspect of a program.
References:
Guide to Process Maturity Models2
What is CMMI? A model for optimizing development processes1
Capability Maturity Model (CMM): A Definitive Guide3
Model-Based Design Notations4
Balanced Scorecard
Project Management Methodologies

NEW QUESTION: 147
□□ □ IT □□ □□□ □□□□□□ □□ □□□ □□□ □□□□□?
A. IT □□□ □□□ □ □□ □□
B. □□ □□□ □□□□ □□ □□ □□□ □□
C. □□ □□□ □□□ □□
D. □□ □□□ □□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 148
□□ □□□□ □□ □□□□ □□ □□ □□□□ □□□ □□ □ □□□ □□□□ □□□ □□□□□ □□□□□ □□□□. □□ □ □□□□ □□ □ □□ □□□ □□□ □□□□ □?
A. □□ □□□□ □□ □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□□□ □□□□□.

C. □□ □□ □□ □□□ □□□ □□□□□.
D. □□ □□□□ □□ □□□ □□□□ □□ □□ □□
Answer: (SHOW ANSWER)
The auditor's best course of action when senior management disagrees with some of the facts presented in the draft audit report is to gather evidence to analyze senior management's objections. The auditor should not revise the assessment, escalate the issue, or finalize the report without changes until they have evaluated the validity and relevance of senior management's objections and resolved any discrepancies or misunderstandings. The auditor should maintain a professional and objective attitude and seek to present a fair and accurate audit report based on sufficient and appropriate evidence. References:
* CISA Review Manual (Digital Version), page 372
* CISA Questions, Answers & Explanations Database, question ID 3338

NEW QUESTION: 149
□□ □□ □□(CSA)□ □□ □□□ □□□ □□□□.
A. □□□ □□□ □□□ □□□ □□ □□□ □□□□□.
B. □□□ □□ □□□ □□□□□□ □□□□□.
C. □□□□ □□□ □□□□ □□ □□□ □□□□□.
D. □□□ □ □□ □□□□ □□□ □□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
The primary objective of a control self-assessment (CSA) is to educate functional areas on risks and controls. CSA is a technique that allows managers and work teams directly involved in business units, functions or processes to participate in assessing the organization's risk management and control processes1. CSA can help functional areas to obtain a clear and shared understanding of their major activities and objectives, to foster an improved awareness of risk and controls among management and staff, to enhance responsibility and accountability for risks and controls, and to highlight best practices and opportunities to improve business performance2.
The other options are not the primary objective of a CSA. Ensuring appropriate access controls are implemented is a specific type of control that may be assessed by a CSA, but it is not the main goal of the technique. Eliminating the audit risk by leveraging management's analysis is not a realistic or desirable outcome of a CSA, as audit risk can never be completely eliminated, and management's analysis may not be sufficient or reliable without independent verification. Gaining assurance for business functions that cannot be audited is not a valid reason for conducting a CSA, as all business functions should be subject to audit, and a CSA is not a substitute for an audit.
References:
Control Self Assessments - PwC
Control self-assessment - Wikipedia
Control Self Assessment - AuditNet

NEW QUESTION: 150
IS □□□□ □□□ □□ □□□ □□□ □□ □□ □□□□ □□□ □□ □□□□ □□ □ □□ □□ □□□□□?
A. □□ □□□ □□□□ □□□□□.
B. □□ □□ □□□(IDS)□ □□□□□.
C. □□□□□□ □□□ □□ □□□ □□ □□□□□□ □□□□□.
D. □□ □□□ □□□ □□□ □□□□□ □□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
Digital watermarks are hidden marks or codes that can be embedded into digital files, such as images, videos, audio, or documents. They can be used to identify the source, owner, or authorized user of the data, as well as to track any unauthorized copying or distribution of the data. Digital watermarks can help prevent data leakage by deterring potential leakers from sharing sensitive data or by providing evidence of data leakage if it occurs.
The other options are not as effective as digital watermarks in preventing data leakage. Ensuring that paper documents are disposed securely can reduce the risk of physical data leakage, but it does not address the digital data leakage that is more prevalent in today's environment. Implementing an intrusion detection system (IDS) can help detect and respond to cyberattacks that may cause data leakage, but it does not prevent data leakage from insiders or authorized users who have legitimate access to the data. Verifying that application logs capture any changes made can help audit and investigate data leakage incidents, but it does not prevent them from happening in the first place.
References:
* What is Data Leakage?
* What is Digital Watermarking?

NEW QUESTION: 151
□□ □ □□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□ □□
C. □□□□ □□(CSA)
D. □□□□ □□□
Answer: (SHOW ANSWER)
Control self-assessment (CSA) is a technique that enables business managers and staff to assess and improve the effectiveness of their own controls and risk management processes. CSA can best enable the timely identification of risk exposure, as it allows for continuous monitoring and reporting of risks by those who are closest to the business processes and activities. External audit review, internal audit review, and stress testing are also useful methods for identifying risk exposure, but they are not as timely as CSA, as they are performed periodically or on demand by external or internal parties who may not

have as much insight into the business operations and environment. References: ISACA CISA Review Manual 27th Edition, page 95.

NEW QUESTION: 152
□□ □□□ Agile □□□□ □□ □□□□ □□□□ □□□ ERP(Enterprise Resource Planning) □□□□ □□□□ □□ □□ □□□□ □□□□ □□□□. □ □□□□ □□□ □ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□
B. □□□ □□ □□□ □□□ □ □□ □□
C. ERP □□ □□
D. Agile □□□□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 153
□□ □□ □□□ □□ □□□ □□□ □□ □□□□□.
A. □□ □□□ □□□□□ □□□□ □□□□□□□.
B. □□□ □□□ □□ □□□ □□□□ □□ □□.
C. □□□ □□□ □□ □□□□ □□□ □□□□□□.
D. □□□ □□□ □□ □□□ □□□ □□□ □□ □□.
Answer: A (LEAVE A REPLY)
The primary advantage of object-oriented technology is enhanced efficiency due to the re-use of elements of logic. Object-oriented technology is a software design model that uses objects, which contain both data and code, to create modular and reusable programs. Objects can be inherited from other objects, which reduces duplication and improves maintainability. Grouping objects into methods for data access, managing sequential program execution for data access, and managing a restricted variety of data types for a data object are not advantages of object-oriented technology. References: ISACA CISA Review Manual 27th Edition, page 304

NEW QUESTION: 154
□□ □□ □□(DRP)□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□□ □□(BCP)
B. □□ □□□ □□ □□□ □□

C. □□ □□ □□□□ □ □□ □□□ □□□ □□
D. □□□ □□□□ □□ □ □□
Answer: D (LEAVE A REPLY)
The most important thing to define within a disaster recovery plan (DRP) is the roles and responsibilities for recovery team members, as this ensures that everyone knows what to do, who to report to, and how to communicate in the event of a disaster. A business continuity plan (BCP) is a broader document that covers the overall strategy and objectives for maintaining or resuming business operations after a disaster. Test results for backup data restoration are important to verify the integrity and availability of backup data, but they are not part of the DRP itself. A comprehensive list of disaster recovery scenarios and priorities is useful to identify the potential risks and impacts of different types of disasters, but it is not as critical as defining the roles and responsibilities for recovery team members.
References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.3: Disaster Recovery Planning1

NEW QUESTION: 155
□□ □ □□□ □□ □□(DLP) □□□ □□□ □□□□ □□□ □□□□ □ □□ □□□□ □□ □□□□□?
A. □□□□ □□□ □□
B. □□ □□ □□
C. □□□ □□□□
D. □□ □□□
Answer: B (LEAVE A REPLY)
Deep packet inspection (DPI) is a core capability of data loss prevention (DLP) tools that allows the analysis of the content of data packets in transit. This helps detect the unauthorized movement of sensitive data by examining packet-level details.
* Network Traffic Logs (Option A): These provide historical data but do not actively detect data in transit.
* Data Inventory (Option C): Useful for identifying where sensitive data resides but not for monitoring its movement.
* Proprietary Encryption (Option D): Protects data but does not detect unauthorized transmission.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 156
□□□ □□ □□□□ □□□□ □ □□ □□□ □□□ □□□□ □□□□.
A. □□□ □□ □ □□ □□ □□
B. □□□□ □□□ □□□ □□
C. □□□ □□ □□□ □□□ □□

D. □□□□ □□ □ □□□ □□□ □□

Answer: (SHOW ANSWER)

The first step in auditing a data communication system is to determine the business use and types of messages to be transmitted. This is because the auditor needs to understand the purpose, scope, and objectives of the data communication system, as well as the nature, volume, and sensitivity of the data being transmitted. This will help the auditor to identify the risks, controls, and audit criteria for the data communication system.
Traffic volumes and response-time criteria, physical security for network equipment, and the level of redundancy in the various communication paths are important aspects of a data communication system, but they are not the first step in auditing it. They depend on the business use and types of messages to be transmitted, and they may vary according to different scenarios and requirements. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 157

□□ □□ □□□ □□□ □ IT □□ □□□□ □□ □□ □□□□ □ □□□ □□□□□?

A. IT □□□ □□□ □□□ □□

B. □□ □□□□ □□ □□ □ □□ □□

C. □□ □□□□ □□

D. □□□ IT □□□□□ □□□□ □□ □□□ □□□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 158

□□ □□□ □□ □□□□ □□□ □□□□ □□□□ □□ □ □□□□ □□□ □□ □ □ □□□□?

A. □□ □□□□

B. □□□□□

C. □□ □ □□□(PKI)

D. □□□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 159

IT □□□ □□□ □□□ □□□□ □□□ □□□□□ □□□□ □□ □□ □□□ □□□□ □?

A. □□□□□□(EVA)

B. □□ □□□(ROI) □□

C. □□ □□

D. □□ □□ □□

Answer: (SHOW ANSWER)

The best method to determine if IT resource spending is aligned with planned project spending is earned value analysis (EVA). EVA is a technique that compares the actual

cost, schedule, and scope of a project with the planned or budgeted values. EVA can help to measure the project progress and performance, and identify any variances or deviations from the baseline plan1.
EVA uses three basic values to calculate the project status: planned value (PV), earned value (EV), and actual cost (AC). PV is the amount of work that was expected to be completed by a certain date, according to the project plan. EV is the amount of work that was actually completed by that date,measured in terms of the budgeted cost. AC is the amount of money that was actually spent to complete the work by that date1.
By comparing these values, EVA can determine if the project is on track, ahead, or behind schedule and budget. EVA can also calculate various indicators, such as cost variance (CV), schedule variance (SV), cost performance index (CPI), and schedule performance index (SPI), to quantify the magnitude and direction of the variances. EVA can also forecast the future performanceand completion of the project, based on the current trends and assumptions1.
The other options are not as effective as EVA in determining if IT resource spending is aligned with planned project spending. Option B, return on investment (ROI) analysis, is a technique that evaluates the profitability or efficiency of an investment, by comparing the benefits or revenues with the costs. ROI analysis can help to justify or prioritize a project, but it does not measure the actual progress or performance of the project against the plan2. Option C, Gantt chart, is a tool that displays the tasks, durations, dependencies, and milestones of a project in a graphical format. Gantt chart can help to plan and monitor a project schedule, but it does not show the actual cost or scope of the project3. Option D, critical path analysis, is a technique that identifies the longest sequence of tasks or activities that must be completed on time for the project to finish on schedule. Critical path analysis can help to optimize and control a project schedule, but it does not account for the actual cost or scope of the project4.
References:
* Earned Value Analysis & Management (EVA/EVM) - Definition& Formulae1
* Return on Investment (ROI) Formula2
* What Is a Gantt Chart?3
* Critical Path Method for Project Management

NEW QUESTION: 160
□□□□ □□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□ □ □□□ □□ □ □□ □□□ □□ □□□□□?
A. □□□□□ □□□ □□□ □□□□□□ □□ □□ □□
B. □□□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□□□.
C. □□ □□□□ □□□□ □□ □□ □□ □□□□□ □□ □□ □□ □□
D. □□□□ □□□ □□□□ □□ □□□□ □3□ □□
Answer: B (LEAVE A REPLY)

The most important factor to ensure that electronic evidence collected during a forensic investigation will be admissible in future legal proceedings is to document evidence handling by personnel throughout the forensic investigation. Documentation is essential to establish the chain of custody, prove the integrity and authenticity of the evidence, and demonstrate compliance with legal and ethical standards. Documentation should include information such as the date, time, location, source, destination, method, purpose, result, and authorization of each action performed on the evidence. Documentation should also include any observations, findings, assumptions, limitations, or exceptions encountered during the investigation. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 161
IS □□□□ □□ □□□ □□ □□ □□ □□□□ □□ □□□□ □□□□ □□□, □□□ □□ □□□ □□□□□ □□ □□□ □□□ □□□□ □□□□. □□□□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□ □□□□ □□□
B. □□□ □□□
C. □□□□ □□□ □ □□□ □□□ □□□
D. □□□ □□□ □□□ □□ □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 162
□□□ □□□ □□□□□ □□ □□□ □□□□□ □□□□□□ □□□□ □□ □□□□ □□□ □□□ □□□□.
A. □□ □□□ □□(ITF).
B. □□ □□□□□.
C. □□ □□.
D. □□□ □□ □□.
Answer: C (LEAVE A REPLY)
Transaction tagging is a technique by which transactions are marked with unique identifiers or headers and traced through the system using agents or sensors at each processing point1. Transaction tagging allows for continuous monitoring and analysis of transaction processing in a high-volume, real-time system by providing visibility into the performance, availability, and reliability of each transaction and its components1. Transaction tagging can also help to identify and isolate errors, bottlenecks, anomalies, and security issues in the system1.

NEW QUESTION: 163
IS □□ □□□ □□□□ □□□ □ □□ □□ □□□ □□□ □ □□ □□□□□?
A. □□□ □□□ □□□□□□ □□ □□□ □□ □□□

B. □□ □□□ □□ □□□ □□□
C. □□ □□ □□ □□□ □□, □□ □ □□
D. □□ □□□ □□ □□□ □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 164
□□ □ □□ □□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□□ □ □□ □□□□□?
A. □□□□
B. □□□
C. □□ □□□
D. □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 165
□□ □ □□□□ □□□ □□□□□□ □□□ □□□□ □ □□ □□□ □□□ □□□□ □?
A. □□□□□ □□□□□□□ □□□□□ □□ □□□ □
B. □□ □□□ □□ □□
C. □□ □ □□□ □□ □
D. □□ □□(QA) □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 166
□□ □ □□□□ □□□ □□ □□□(CASB)□ □□□ □□□□□ □□□□ □□□□ □□ □□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□□
B. □□ CASB □□ □□
C. □□□□□□ □□
D. □□□ □□□ □□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
ACloud Access Security Broker (CASB)ensuresvisibility, compliance, and securityof cloud applications, andmonitoring data movementis the key to detecting threats.
* Option A (Correct):Monitoring data movementallows organizations todetect and prevent unauthorized access, data exfiltration, and cloud-based threats.
* Option B (Incorrect):Along-term contractdoes not inherentlyimprove security monitoring.
* Option C (Incorrect):Reviewing policies helps withgovernance, but it does notactively detect threats.
* Option D (Incorrect):Firewallsprotectnetwork perimeters, while CASBs focus oncloud security, making this anineffective measurefor CASB threat detection.

Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-CoversCASB, cloud security, and threat detection best practices.

NEW QUESTION: 167
IT □□□ □□□□□□ □, □□□ □□ □□□□□□ □□ □ □□□ □□□□ □□ □□ □□□?
A. □□ □□□ □ □□□□ □□□ □□□□□ □□□ □ □□□□.
B. □□ □□ □□□□□ □□□□□ □□□□□ □□□□□.
C. □□□ □□□ □□ □□□□□ □□□□ □□□□□□□.
D. □□ □ □□□□ □□ □□□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:Unauthorized data modifications during conversion (D) are the most critical concern because they compromise data integrity, leading to inaccurate or corrupted information in the new system. Data migration should be performed with strict controls, including validation, reconciliation, and audit trails.
Other options:
* Lack of online backups (A) is a risk but not as severe as compromised data integrity. Offline backups may still exist.
* Undocumented change management (B) is a process deficiency but does not directly affect data accuracy.
* Manual data conversion (C) increases risk but does not automatically indicate unauthorized changes.
Reference: ISACA CISA Review Manual, Information Systems Acquisition, Development, and Implementation

NEW QUESTION: 168
□□ □ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□ □□□□□ □□□□ □ □□ □□□□□?
A. □□□□ □□□ □□□□ □□ □ □□□□□ □□□□ □□□□.
B. □□□□ □□ □□□ □□□□ □□□□□.
C. □□□ □□□□ □□□□ □□□□□□ □□□□ □□ □□□□□.
D. □□□□ □□□ □□ □□□ □□□□ □□□.
Answer: D (LEAVE A REPLY)

Data leakage prevention (DLP) is the process of preventing unauthorized access, disclosure, or transfer of sensitive data. In a multi-tenant cloud environment, where multiple customers share the same infrastructure and resources, DLP is a critical challenge. One of the best methods to enforce DLP in such an environment is to require tenants to implement data classification policies. Data classification policies define the types and levels of sensitivity of data, and the corresponding security controls and measures to protect them. By implementing data classification policies, tenants can ensure that their data is properly labeled, encrypted, segregated, and monitored according to their specific requirements and compliance standards. This can help prevent data leakage from accidental or malicious actions by other tenants, cloud service providers, or external parties.
References:
* 2: How Do I Secure my Data in a Multi-Tenant Cloud Environment? | Thales
* 3: Protecting Sensitive Customer Data in a Cloud-Based Multi-Tenant Environment | Saturn Cloud
* 4: Microsoft 365 isolation controls - Microsoft Service Assurance

NEW QUESTION: 169
□□□ □□□ □□ □□ □□□□(CCTV) □□ □□□□ □□□ □□ □□ □ IS □□□□ □□ □□□□ □□ □□ □□□□□?
A. CCTV □□ □□□ □□□□□ □□□□ □□□□.
B. □□□□ CCTV □□□□ □□□□ □□ □□□□.
C. CCTV □□□ 1□ □ □□□□□.
D. CCTV □□□ 24□□ □□ □□□□ □□□□.
Answer: (SHOW ANSWER)
The most concerning issue associated with a data center's CCTV surveillance cameras is that the recordings are not regularly reviewed. This means that any unauthorized access, theft, vandalism, or other security incidents may go unnoticed and unreported. CCTV recordings are a valuable source of evidence and deterrence for data center security, and they should be monitored and audited periodically to ensure compliance with policies and regulations. If the recordings are not reviewed, the data center may face legal, financial, or reputational risks in case of a security breach or an audit failure.
The other options are less concerning because they do not directly affect the security of the data center. CCTV cameras are not required to be installed in break rooms, as they are not critical areas for data protection.
CCTV records can be deleted after one year, as long as they comply with the data retention policy of the organization and the applicable laws. CCTV footage does not need to be recorded 24 x 7, as long as there is sufficient coverage of the data center during operational hours and when access is granted to authorized personnel. References:
* ISACA Journal Article: Physical security of a data center1
* Data Center Security: Checklist and Best Practices | Kisi2

* Video Surveillance Best Practices | Taylored Systems

NEW QUESTION: 170
□□ □ □□□□ □□□ □□(BCP)□ □□ □□□ □□□□□ □□□□ □□□ □□ □□ □ □□□□ □□ □□□□□?
A. □□□□ □□□ □□
B. □□□□ □□□ □□
C. □□□□□ □□□ □□
D. □□ □□ □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 171
□□ □□□□□ □□□ □□□□ □□ □ □□ □□□ □□ □□□□□?
A. □□□ □□□□ □□□ □□□□□ □□ □□
B. □□ □□□□□ □□ □□ □□
C. □□□ □□ □□□□ □3□□ □□□ □
D. □□ □□□□□ □□□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 172
□□□□ □□□ □□ □□ □□□□ □□□□ □□□ □□ □□□□ □□□□□. □□ □ □□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□□□ □□ □□□ □□□□□.
B. □□ □□□(VPN)□ □□ □□ □□□□ □□□ □□□□□.
C. □□ □□□□□ □□□□ □□□□ □□□□□.
D. □□ □□□□ □□□□ □□□ □□□ □□ □□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 173
□□ □ □□□ □□ □□□ □□□□ □ □□ □□ □□□ □□□□□?
A. □□□□ □□ □□ □□
B. □□□□□□ □□ □□
C. □□ □□ □□ □□□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 174
□□ □□ □□ IS □□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□ □ □□□□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□□□ □□ □□ □□□ □□□□□.
B. □□ □□□□□ □□□□□ □□□ □□□□□.

C. □□ □□ □□□ □□ □□□ □□□□ □□□□□.
D. □□ □□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 175
□□□ □□ □□□□ □□ □□ □□□ □□□ □ □□□ □□□□ IS □□□□□ □□ □ □□ □□□□ □□□□ □□□ □□ □□□ □□□□□. □□□□ □□□□□ □□□ □□ □ □□□ □□□□□?
A. □□□ □□ □□ □□□□ □□□ □□□□□.
B. □□□□ □□ □□□□ □□ □□ □□□ □□□□.
C. □□□□ □□ □□□□ □□□ □□□□□.
D. □□□ □□ □ □□ □□□□□□ □□□□□□.
Answer: D (LEAVE A REPLY)
A risk and control framework is a set of principles, processes, and tools that guide an organization in identifying, assessing, managing, and monitoring the risks and controls that affect its objectives and performance. A risk and control framework helps an organization to align its risk appetite and tolerance with its strategy, culture, and values, and to ensure that its security controls are appropriate, effective, and efficient1.
Re-evaluating the organization's risk and control framework is the best recommendation to management because it can help them to:
Review the current risk environment and the sources, causes, and impacts of potential threats and vulnerabilities.
Update the risk assessment and analysis methods and criteria, such as likelihood, impact, severity, and priority.
Reconsider the risk response and treatment options, such as avoidance, reduction, transfer, or acceptance.
Realign the security controls with the risk profile and the business needs and expectations.
Evaluate the performance and effectiveness of the security controls using key indicators and metrics.
Identify the gaps, weaknesses, or inefficiencies in the security controls and implement corrective or improvement actions.
Communicate and report the risk and control status and results to relevant stakeholders.
Re-evaluating the organization's risk and control framework can help management to determine whether the current security controls are excessive or not, and to make informed and rational decisions on how to adjust them accordingly.

NEW QUESTION: 176
□□□□□□□□ □□ □□ □□□□□ □□□ □□□ □□□ □ □□□□ □□ □□□□ □□□ □□ □ □□□□□?
A. □□□□□ □□ □□□ □□□□ □□□□□ □□□□□□□ □□ □□□□□.
B. □□□□□□□ □□ □□□ □□, □□ □□□ □□□□ □□□□.

C. □□□ □□□ □□ □□□ 2□ □□ □□□□□ □□□□□□ □□□□□.
D. □□□□□□□ □□□□□ □□ □□□□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)
The auditor's greatest concern when reviewing data inputs from spreadsheets into the core finance system would be undocumented code that formats data and transmits directly to the database. This is because undocumented code can introduce errors, inconsistencies, and security risks in the data processing and reporting. Undocumented code can also make it difficult to verify the accuracy, completeness, and validity of the data inputs and outputs, as well as to trace the source and destination of the data. Undocumented code can also violate the principles of segregation of duties, as the same person who creates the code may also have access to the data and the database.
The other options are not as concerning as undocumented code, although they may also pose some risks. A lack of complete inventory of spreadsheets and inconsistent file naming may make it challenging to identify and locate the relevant spreadsheets, but they do not directly affect the quality or integrity of the data inputs.
The department data protection policy not being reviewed or updated for two years may indicate a lack of awareness or compliance with the current data protection regulations, but it does not necessarily imply that the data inputs are compromised or inaccurate.
Spreadsheets being accessible by all members of the finance department may increase the risk of unauthorized or accidental changes to the data, but it can be mitigated by implementing access controls, password protection, and audit trails.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2261
Five Common Spreadsheet Risks and Ways to Control Them2
GREATEST Concerns When Reviewing Data Inputs from Spreadsheets3

NEW QUESTION: 177
□□ □□□ □□□□ □□□ □□ □□□ □□□ □□ □□, □□ □□ □□ □ □□ □□□ □ □□ □□ □□□ □□ □□□□?
A. □□□□□ □ □□□□□
B. □□ □ □□
C. □□□□ □□ □ □□ □□
D. □□□ □□□ □ □□
Answer: (SHOW ANSWER)
The greatest segregation of duties conflict would occur if the individual who performs the related tasks also has approval authority for purchase requisitions and purchase orders. This is because these two tasks are directly related to each other and involve financial transactions. If the same person is responsible for both tasks, it could lead to potential fraud or error12. For instance, the individual could approve a purchase order for a personal need and then also approve the payment for it, leading to misuse of company funds12.
References:

Segregation of Duties: Examples of Roles, Duties & Violations - Pathlock Functions in the Purchasing Process and how to Segregate Purchasing Duties

NEW QUESTION: 178
IS □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□□ □□ □ □□ □□□ □□□□ □□ □□□ □□ □□ □□□(IDS)□ □□□□ □□□□.
A. □□□ □ □□.
B. □□□□□(DMZ).
C. □□□.
D. □□□ □□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 179
□□ □□ □□□ □□□ □□□ □□□□□ □□□ □□□□ □□ □□□ □□ □□□ □ □ □□□□ □□□□?
A. □□ □□
B. □□ □□□
C. □□□ □□□□ □□□
D. □□□ □□ □□ □□
Answer: D (LEAVE A REPLY)
Recovery facilities providing a redundant combination of Internet connections to the local communications loop is an example of last-mile circuit protection. Last-mile circuit protection is a type of telecommunications continuity that ensures the availability and redundancy of the final segment of the network that connects the end-user to the service provider. The local communications loop, also known as the local loop or subscriber line, is the physical link between the customer premises and the nearest central office or point of presence of the service provider. Byhavingmultiple Internet connections from different providers or technologies, such as cable, DSL, fiber, wireless, or satellite, the recoveryfacilities can avoid losing connectivity in case one of the connections fails or is disrupted by a disaster5.
References:
* 9: Last Mile Redundancy - How to Ensure Business Continuity - Multapplied Networks

NEW QUESTION: 180
□□ □□□ □□ □ □□ □□□ □□ □□□□□ □□□ □ □□ □□ □□□□□?
A. □□ □□□□□
B. □□□□□□ □□ □□□□□
C. □□ □□□ □□□
D. □□□□ □□□
Answer: (SHOW ANSWER)

The type of firewall that provides the greatest degree of control against hacker intrusion is an application level gateway. A firewall is a device or software that filters or blocks network traffic based on predefined rules or policies. A firewall can help protect an information system or networkfrom unauthorized access or attack by hackers or other malicious entities. An application level gateway is a type of firewall that operates at the application layer of the network model (layer 7), which is where user applications communicate with each other over the network. An application level gateway provides the greatest degree of control against hacker intrusion, by inspecting and analyzing the content and context of each network packet at the application level, such as protocols, commands, requests, responses, etc., and allowing or denying access based on specific criteria or conditions. An application level gateway can also perform additional functions such as authentication, encryption, caching, logging, etc., to enhance the security and performance of network traffic.
A circuit gateway is a type of firewall that operates at the transport layer of the network model (layer 4), which is where data are transferred between end points over the network. A circuit gateway provides a moderate degree of control against hacker intrusion by establishing a secure connection between two end points (such as client and server) and relaying network packets between them without inspecting or analyzing their content. A circuit gateway can also perform functions such as encryption, authentication, or address translation to improve the security and privacy of network traffic. A packet filtering router is a type of firewall that operates at the network layer of the network model (layer 3), which is where data are routed between different networks or subnets. A packet filtering router provides a low degree of control against hacker intrusion by examining the header of each network packet and allowing or denying access based on basic criteria such as source address, destination address, port number, protocol, etc. A packet filtering router can also perform functions such as routing, forwarding, or address translation to optimize the delivery and efficiency of network traffic. A screening router is a type of firewall that operates at the network layer of the network model (layer 3), which is where data are routed between different networks or subnets. A screening router provides a low degree of control against hacker intrusion by examining the header of each network packet and allowing or denying access based on basic criteria such as source address, destination address, port number, protocol, etc. A screening router can also perform functions such as routing, forwarding, or address translation to optimize the delivery and efficiency of network traffic.

NEW QUESTION: 181
□□□□□□ □□□(DBA)□ □□□ □□ □□ □□□ □□□ □□□□ □ □□□.
A. □□ □□□ □□□ □□
B. □□□ □□□ □□□□
C. □□□□ □□□ □□ □□□ □□□ □□
D. □□ □□□ ID □□

Answer: A (LEAVE A REPLY)
A database administrator (DBA) should be prevented from having end user responsibilities to avoid a conflict of interest and a violation of the principle of segregation of duties. End user responsibilities may include initiating transactions, authorizing transactions, recording transactions or reconciling transactions. A DBA who has end user responsibilities may compromise the integrity, confidentiality and availability of the data and the database systems. Accessing sensitive information, having access to production files and using an emergency user ID are not end user responsibilities, but rather potential risks or controls associated with the DBA role. References:
* : Database Administrator (DBA) Definition
* : Segregation of Duties | ISACA
* : [End User Definition]

NEW QUESTION: 182
□□□□ □□□□□□ □□□□□ □□□□ □□□ □□ □□□ □□□□ □□□.
A. □□□ □□ □□□□□ □□□□□.
B. □□□ □□□ □□□□□.
C. □□-□□ □□□ □□□□□.
D. □□ □□□(RFP)□ □□□□□.
Answer: C (LEAVE A REPLY)
An organization considering the outsourcing of a business application should first conduct a cost-benefit analysis to evaluate the feasibility, viability and desirability of the outsourcing decision. A cost-benefit analysis should compare the costs and benefits of outsourcing versus keeping the application in-house, taking into account factors such as financial, operational, strategic, legal, regulatory, security and quality aspects. A cost-benefit analysis should also identify the risks and opportunities associated with outsourcing, and provide a basis for defining the service level requirements, performing a vulnerability assessment, and issuing a request for proposal (RFP) in the subsequent stages of the outsourcing process. References: Info Technology
& Systems Resources | COBIT, Risk, Governance ... - ISACA, CISA Certification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 183

□□□ □□□□□ □□□□ □□□□□□ □□□ □□□□ IS □□□□ □□□□□□ □ □□□ □□ □□□□ □□□□□□. □□ □ IS □□□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□□□□.
B. □□ □□□ □□ □□□□□ □□□□□.
C. □□□□ □□ □□□ □□□□□.
D. □□□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
When an IS auditor discovers a security weakness in the database configuration, the next course of action should be to identify existing mitigating controls. This involves assessing whether any controls are already in place to address the weakness and mitigate the risk. Understanding the current state of controls helps the auditor determine the severity of the issue and whether additional corrective actions are necessary1. References: 1(https://www.isaca.org/resources/insights-and-expertise/audit-programs-and-tools)

NEW QUESTION: 184
□□□□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□ □ □□□□□□. IS □□□□ □□□□ □ □□ □□□ □□□□□ □□□□ □□ □□ □ □ □□□ □□□□ □□□□. □□ □ □□ □□□ □ □□ □□ □□ □□□ □□□□□?
A. □□□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□□□□ □□□□ □□□□□□□ □□□□□ □□ □□□.
C. □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□.
D. □□□□□□□ □□ □□□ □□ □□ □□ □□ □□
Answer: C (LEAVE A REPLY)
The most reliable follow-up procedure to determine if management has resolved the finding of non-sequential purchase order numbers is to inspect the system settings and transaction logs to determine if sequential order numbers are generated. This will provide direct evidence of the system's functionality and compliance with the audit recommendation. The other options are less reliable because they rely on indirect evidence or information obtained from management, which may not be accurate or complete. References: CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

NEW QUESTION: 185
IS □□□□ □□□ □□□ □□ □□(DLP) □□□ □□□ □□□ □□□□ □□ □□□ □ □□ □□□ □□ □ □□□□□?
A. □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
B. □□ □□□ □□□□ □□ DLP □□□□□□ □□□□ □□□ □□□□□.
C. □□□ □□ □□□□ □□□□ □□ □□□□ □□□□□.
D. □□ □□□ □□ USB □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

The most reliable way for an IS auditor to evaluate the operational effectiveness of an organization's data loss prevention (DLP) controls is to verify that confidential files cannot be transmitted to a personal USB device. This is because DLP controls are designed to prevent the loss, leakage or misuse of sensitive data through breaches, ex-filtration transmissions and unauthorized use1. A personal USB device is a common way for data to be stolen or compromised, as it can bypass network security measures and allow unauthorized access to confidential files. Therefore, testing the DLP controls by attempting to copy or transfer confidential files to a personal USB device can provide a direct and objective evidence of whether the DLP controls are working as intended or not.
The other options are less reliable ways for an IS auditor to evaluate the operational effectiveness of an organization's DLP controls. Reviewing data classification levels based on industry best practice is a way to assess the adequacy of the organization's data protection policies, but it does not measure how well the DLP controls are implemented or enforced in practice. Verifying that current DLP software is installed on all computer systems is a way to check the technical configuration of the DLP solution, but it does not test how well the DLP software detects and prevents data loss incidents in real scenarios. Conducting interviews to identify possible data protection vulnerabilities is a way to gather qualitative information from stakeholders, but it does not provide quantitative or empirical data on the actual performance of the DLP controls.
References:
What is Data Loss Prevention (DLP)? [Guide] - CrowdStrike

NEW QUESTION: 186
□□□□□ □□□ □□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□ □□ □□ □□ □□□ □□ □ □□ □□□?
A. □□ □□□
B. □□□ □□□
C. □□ □□ □□ □□□
D. □□ □□□
Answer: D (LEAVE A REPLY)
Discovery sampling is a type of statistical sampling that's used when the expected error rate in the population is very low1. This method is designed to discover at least one instance of an attribute or condition in a population1. It's often used in auditing to uncover fraud or noncompliance with rules and regulations1.
References:
What are sampling methods and how do you choose the best one?

NEW QUESTION: 187
□□ □ □□ □□(QA) □□□ □□□□ □ □□ □ □□□ □ □ □□ □□ □□□ □□□ □□?
A. □□ □□□ □□□□ □□□□ □□ □□□ □□ □□□□□ □□□ □□□ □□□□.

B. □□ □□□ □□□□ □□ □□ □□□□ □□ □□□□ □□ □□□ □□□□□.
C. □□ □ □□ □□□□ □□□□ □□□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
A strongQA functionrequires anindependentreview of changes toavoid biasandensure objectivity.
* Option A (Correct):Ifdevelopers review their own changes, there is ahigh risk of biasand overlooking issues, making this the greatest concern. This violatesseparation of dutiesandbest practices for quality assurance.
* Option B (Incorrect):Peer reviews within the same teamreduce risksincefresh eyesreview the changes, though it is not as strong as an external review.
* Option C (Incorrect):Havingdevelopers from a separate teamreview the code providesbetter objectivityand reduces risks associated withself-review.
* Option D (Incorrect):Whilenon-developers may lack technical expertise, their review ensuresindependence, making it a stronger control than self-review.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversquality assurance, code reviews, and segregation of duties.

NEW QUESTION: 188
IS □□□□ IT □□□ □□□ □ □□ □ □□ □□□□ □ □□□ □□□□□?
A. □□ □□□□ □□□□□□□ □□ □□ □□□□ □□□□□ □□□□ □□□□□.
B. □□ □□□□ □□□□□□□ □□ □□□□ □□ 2□□ □□□□ □□□□ □□□□ □.
C. □□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □ □□□□ □□□□.
D. □□ □□□□ □□□□□□ □□□□□ □□ □□□ □□ □□□□ □□ □□ □ □□ □□ □□□□□.
Answer: (SHOW ANSWER)
Changes to the job scheduler application's parameters are not approved and reviewed by an operations supervisor. This is a serious control weakness that could compromise the integrity, availability, and security of the IT operations. An IS auditor should be concerned about the lack of oversight and accountability for such changes, which could result in unauthorized, erroneous, or malicious modifications that affect the processing environment. The other options are less critical issues that may not have a significant impact on the IT operations. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.11
* CISA Review Questions, Answers & Explanations Database, Question ID 202

NEW QUESTION: 189
□□ □□□ □□□ □□ □□□□ □□□ □□□□ □□□ □ □□□ □□□.

A. □□ □□□□ □□ □□□ □□□□□□□.
B. □□ □□□□ □□□ □□□□□.
C. □□□□ □□ □□□ □□□□□□□.
D. □□□ □□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
The business case for an information system investment is a document that provides the rationale and justification for the investment, based on the expected costs, benefits, risks, and impacts of the project12. The business case should be available for review until the benefits have been fully realized, because it serves as a baseline for measuring the actual performance and outcomes of the project against the planned ones34. This helps to evaluate the success and value of the investment, and to identify any gaps or issues that need to be addressed5.
References
1: The Business Case for Security - CISA
2: Beyond the Business Case: New Approaches to IT Investment
3: #HowTo: Build a Business Case for Cybersecurity Investment
4: ISACA CISA Certified Information Systems Auditor Exam ... - PUPUWEB
5: The Business Case for Security | CISA

NEW QUESTION: 190
□□□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□ □□□ □□
B. □□□□ □□□□ □□ □□
C. □□□ □□ □□
D. □□□ □□□ □□ □□□□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
IS □□□□ □□□ IT □□□ □□ □□□ □□ □□□□ □□ □□, IT □□□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□ □□ □□□□□□. □□ □□ □ □□ □□ □□ □□□ □□□□□?
A. IT □□□ □□□□ □□□ □□ □□□□□.
B. IT □□□□□□ □□□□ □□
C. □□□ □□□□ □□□□ □□ IT □□□ □□□□□.
D. IT □□□□□□ IT □□□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
The best recommendation is to align the IT strategy with the business objectives. This will ensure that the IT projects and initiatives are consistent with the organization's vision, mission, and goals. IT strategy should be derived from and support the business strategy, not the other way around. By aligning the IT strategy with the business objectives, the organization can achieve better value, performance, and alignment from its IT investments.

Reviewing priorities in the IT portfolio (option B) is not the best recommendation, as it does not address the root cause of the misalignment between the IT strategy and the IT portfolio. The IT portfolio should reflect the IT strategy, which in turn should reflect the business objectives. Simply changing the priorities in the IT portfolio without aligning the IT strategy with the business objectives may result in suboptimal or conflicting outcomes.
Changing the IT strategy to focus on operational excellence (option C) is also not the best recommendation, as it may not be aligned with the business objectives. The organization's IT strategy should be based on its competitive advantage, market position, customer needs, and industry trends. If the organization's business strategy is heavily focused on research and development, then changing the IT strategy to focus on operational excellence may not be appropriate or beneficial.
Aligning the IT portfolio with the IT strategy (option D) is also not the best recommendation, as it does not address the misalignment between the IT strategy and the business objectives. Aligning the IT portfolio with the IT strategy may improve the coherence and consistency of the IT projects, but it may not ensure that they are aligned with the organization's vision, mission, and goals.
Therefore, option A is the correct answer.
References:
* The Challenges of Aligning IT and the Business | CIO Insight
* Strategic alignment and value maximization for IT project portfolios ...
* A Guide to IT Portfolio Management | Adobe Workfront

NEW QUESTION: 192
IS □□□□ □□□ □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□. □□ □□□ □ □□ □□□ □ □□ □□□ □□□□ □□ □□□□□?
A. □□□ □□□
B. □□□ □□ □□□
C. □□ □□□
D. □□ □□ □□□
Answer: D (LEAVE A REPLY)
Compliance testing ensures that the organization's incident response processes align with established cybersecurity frameworks and policies. This methodology provides objective and reliable conclusions about the maturity of incident response capabilities.
* Judgmental Sampling (Option A):Relies on subjective judgment and is less reliable.
* Data Analytics Testing (Option B):Useful for identifying trends but may not assess process maturity comprehensively.
* Variable Sampling (Option C):Appropriate for statistical analysis but less effective in process maturity assessments.
Reference:ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

NEW QUESTION: 193
□□□ IT □□□ DevOps□ □□□□□, □□ □□ □ □□□ □□□□ □□□□□ □□□ □□□□ □□□□ □□□□□ □□ □□ □□ □□□□ □□□ □ □□□□. □□ □ □□ □□□□ □□□ □□□□□?
A. □□□ □□□□ □□ □ □□□□ □□ □□ □□□ □□□ □□□□□.
B. DevOps □□ □□□ □□□ □□□□ □□□□ □□□□ □□□ □□ □□□ □□ □□ □□□.
C. □□ □□□ □□ □□□□ □□□ □□ □□□ □□□□ □ □□□□ □□□□□.
D. IT □□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The most effective control to maintain segregation of duties in a DevOps environment is A. Enforce approval prior to deployment by a member of the team who has not taken part in the development. Segregation of duties (SoD) is a principle that requires multiple actors to complete a task to reduce the risk of fraud, error, or abuse1. In a DevOps environment, where developers and operators work together to deliver software faster and more reliably, SoD may seem to be incompatible or impractical. However, SoD can still be achieved by implementing controls that ensure that no single person can develop, test, and deploy code without oversight or review2.
Enforcing approval prior to deployment by a member of the team who has not taken part in the development is an effective control that ensures that code changes are verified and validated by a peer before they are released to production. This control can help prevent or detect any unauthorized or malicious modifications, errors, or vulnerabilities in the code, and ensure that the code meets the quality and security standards3. This control can also promote collaboration and feedback among the team members, and improve the transparency and accountability of the software delivery process3.

NEW QUESTION: 194
□□ □□□ □□□□□□ □□□□□ ERP(Enterprise Resource Planning) □□□□ □□ □□□□□ 2□ □□□□□ □□ □□□, 1□□□□ □□□ □□ □□□□□□ □□□□ 2 □□□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□□□ □□□□□ □□□□ □. IS □□□□ □□ 2□□□ □□□ □ □□ □□□□□ □□□□ □ □□□ □□ □ □□ □□□□?
A. □□□ □□□□□□
B. □□□ □□□
C. □□□ □□ □□□(UAT)
D. □□ □□□ □□□ □□□□□
Answer: (SHOW ANSWER)
During the second year of the ERP system upgrade project, the focus shifts to ensuring that the updated business processes integrate seamlessly with the new system

functionality. User acceptance testing (UAT) validates that the system meets user requirements and business objectives.
* Data Migration (Option A): Data migration is more relevant in the first phase when upgrading the system version.
* Sociability Testing (Option B): This is less critical than confirming user functionality for process changes.
* Initial User Access Provisioning (Option D): This is part of security and access controls but not the primary focus of business process validation.
Reference: ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 195
□□ □ □□ □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□
D. □□ □□
Answer: (SHOW ANSWER)
The primary basis on which audit objectives are established is the consideration of risks12. This involves identifying and assessing the risks that could prevent the organization from achieving its objectives12. The audit objectives are then designed to address these risks and provide assurance that the organization's controls are effective in managing them12. While audit risk, assessment of prior audits, and business strategy are important factors in the audit process, they are secondary to the fundamental requirement of considering risks12.
References:
Objectives of Auditing - Primary and Secondary Objectives of Auditing | Auditing Management Notes Audit Objectives | Primary and Subsidiary Audit Objectives - EDUCBA

NEW QUESTION: 196
□□ □□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□ □□□□ □□□ □□□ □□□□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□□ □ □□□□ □□□ □□□ □□□□□.
C. □□□□ □□□□ □□□□ □□□ □□ □□ □□□ □□□□□□.
D. □□ □□□ □□ □□□□□□.
Answer: D (LEAVE A REPLY)
Deferring remediation testing until the next audit is justified only when there are significant changes in the audit environment that affect the relevance or validity of the audit observations and recommendations. For example, if there are changes in the business processes, systems, regulations, or risks that require a new audit scope or approach. The other options are not valid justifications for deferring remediation testing, as they do not

address the timeliness or quality of the audit follow-up process. The auditor who conducted the audit and agreed with the timeline has left the organization does not affect the responsibility of the audit function to ensure that remediation testing is performed as planned. Management's planned actions are sufficient given the relative importance of the observations does not guarantee that management will actually implement those actions or that they will be effective in addressing the audit issues. Auditee management has accepted all observations reported by the auditor does not eliminate the need for verification of remediation actions by an independent party. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION: 197
□□□□ □□□□□□ □□ □ □□□ □□ □□ □□□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□ □ □□ □□□ □□□ □□□ □□ □ □□□□□?
A. □□□□□□ □□□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
B. □□□□□ □□□ □□□ □□ □□ □□□□□.
C. 25□ □□□ □□ □ □□□ □□ □□□ □□□ □□□□□.
D. □ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The most appropriate testing approach when auditing a daily data flow between two systems via an automated interface is to perform data reconciliation between the two systems for a sample of 25 days. Data reconciliation is a process of verifying that the data transferred from one system to another is complete and accurate, and that there are no discrepancies or errors in the data flow1. Data reconciliation can be performed by using generalized audit software, which is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases2. By performing data reconciliation for a sample of 25 days, the IS auditor can test the reliability and consistency of the data flow over a reasonable period of time, and identify any potential issues or anomalies that could affect the quality of the data or the functionality of the systems.
References
1: Data Flow Testing - GeeksforGeeks 2: Generalized Audit Software (GAS) - ISACA

NEW QUESTION: 198

□□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□□ □□ □□□□ □□ □□□ □□□□ □□□?

A. □□ □□□ □□□□ □□ □□ □□□ □□□ □□

B. □□ PIN □□ □□

C. □□□□ □□ □□□ □□□□ □□□ □□

D. □□□□ □□□□(CCTV) □□

Answer: (SHOW ANSWER)

Periodic review of access profiles by management is an additional control that is required when using swipe cards to limit employee access to restricted areas. Swipe cards are a type of physical access control that use magnetic stripes or radio frequency identification (RFID) to store and transmit information about the cardholder's identity and access rights. Swipe cards can help to prevent unauthorized entry, protect sensitive assets and data, and monitor access activity. However, swipe cards alone are not enough to ensure effective access control. They need to be complemented by other controls, such as:

Periodic review of access profiles by management: This is a type of logical access control that involves verifying that the access rights assigned to each cardholder are appropriate, necessary, and consistent with the organization's policies and procedures. Periodic review of access profiles can help to detect and correct any errors, inconsistencies, or violations in the access control system, such as outdated, excessive, or redundant access rights, segregation of duties conflicts, or unauthorized changes. Periodic review of access profiles can also help to ensure compliance with internal and external audit requirements and regulations.

Implementation of additional PIN pads: This is a type of multi-factor authentication (MFA) that requires the cardholder to enter a personal identification number (PIN) in addition to swiping their card. MFA can enhance the security of the access control system by adding another layer of verification and reducing the risk of lost, stolen, or cloned cards being used by unauthorized persons.

Installation of closed-circuit television (CCTV): This is a type of surveillance system that uses cameras and monitors to record and display the images of the people and activities in the restricted areas. CCTV can deter potential intruders, provide evidence of any security incidents or breaches, and enable real-time monitoring and response by security personnel.

The other options are not as effective or relevant as periodic review of access profiles by management for an additional control when using swipe cards. Physical sign-in of all employees for access to restricted areas is a redundant and inefficient control that can be easily bypassed or manipulated. It also does not provide any assurance or verification of the identity or access rights of the cardholders. Audit hooks are software routines embedded in an application that can trigger an alert or a report when certain conditions are met. Audit hooks can help to detect anomalies or exceptions in access control lists, but they do not provide a comprehensive or integrated view of them.

References:

ISACA, CISA Review Manual, 27th Edition, 2019, p. 236
ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, p. 88 Data Analytics for Auditing Access Control

NEW QUESTION: 199
□□ IT □□□□□□ □□□ □□□ □□ □□ □□□ □□□□ □, IS □□□□ □□ □□ □□□ □□ □ □□ □□ □□ □□□□ □□ □ □□ □□□?
A. □□□□ □□□ □□ □□ IT □□□□□□ □□□□□.
B. □□□□ □□□ □□ □□ IT □□□□□□ □□□□□□.
C. IT□ □□ □□ □□(KPI)□ □□□□□.
D. IT □□□□□□ □□ □□ □□□(ROI)□ □□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 200
□□ □□□ □□□ □□□□□ □□□ □□□□□□. □□ □ □□ □□ □□□ □□□□ □ □□□ □□□ □□□□ GREATE ST □□□□□?
A. □3□□ □□ □□□ □□□ □□ □□□□□□.
B. □□□ □□ □□ □□□ □□□ □□
C. □□□ □□□ □□□ □□
D. □□ □□ □□□ □□ □□□□□□.
Answer: C (LEAVE A REPLY)
The greatest indicator that the cybersecurity policy may need to be revised is a significant increase in approved exceptions. This implies that the policy is not aligned with the current business needs and risks, and that it may be too restrictive or outdated. The other options are not necessarily indicators of a need for policy revision, as they may be due to other factors such as changes in the external environment, audit scope or methodology.
References: CISA Review Manual (Digital Version), Chapter 5, Section 5.21

NEW QUESTION: 201
IT □□□□□ □□□ □□□ □□, □□□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□□□ □□□□□ □□ □□□ □□□□□□. □□ □ IS □□□□ □□ □□ □□ □□ □ □□□□□?
A. □□□ □ □□□□ □□□□ □□□□ □□□□□□ □□□□□.
B. □□□ □ □□□ □ □□□ □□□ □□□□□□.
C. □□□ □□□ □□ □□□, □□□ □ □□ □□□ □□□□□□.
D. □□□ □□□ □ □□□□ □□□□ □□□□□ □□□.D
Answer: (SHOW ANSWER)

NEW QUESTION: 202
□□□ □□ □□□ □□ □□□□ □□□□□ □□□□ □□□□□□□ □□□. □□ □ □□ □□□ IS □□ □□ □□□ □□□□□?

A. □□□ □□□□ □□ □□□□□ □□□□.
B. □□□□□ □□ □□ □□□□ □□ □□ □□□ □□□□□ □□□□□.
C. □□□□ □□ □□□ □□ □□□ □□□□ □□□ □□□ □□ □□□□□.
D. □□□□ □□ □□ □□□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
A post-implementation review (PIR) is a process to evaluate whether the objectives of the project were met, determine how effectively this was achieved, learn lessons for the future, and ensure that the organisation gets the most benefit from the implementation of projects1. A PIR is an important tool for assessing the success and value of a project, as well as identifying the areas for improvement and best practices for future projects.
One of the key elements of a PIR is to measure the benefits of the project against the expected outcomes and benefits that were defined at the beginning of the project. Measurable benefits are the quantifiable and verifiable results or outcomes that the project delivers to the organisation or its stakeholders, such as increased revenue, reduced costs, improved quality, enhanced customer satisfaction, or compliance with regulations2. Measurable benefits should be aligned with the organisation's strategy, vision, and goals, and should be SMART (specific, measurable, achievable, relevant, and time-bound).
The finding that measurable benefits were not defined is of greatest significance among the four findings, because it implies that:
* The project did not have a clear and agreed-upon purpose, scope, objectives, and deliverables
* The project did not have a valid and realistic business case or justification for its initiation and implementation
* The project did not have a robust and effective monitoring and evaluation mechanism to track its progress, performance, and impact
* The project did not have a reliable and transparent way to demonstrate its value proposition and return on investment to the organisation or its stakeholders
* The project did not have a meaningful and actionable way to learn from its achievements and challenges, and to improve its processes and practices Therefore, an IS auditor should recommend that measurable benefits are defined for any project before its implementation, and that they are reviewed and reported regularly during and after the project's completion.
The other possible findings are:
* A lessons-learned session was never conducted: This is a significant finding, but not as significant as the lack of measurable benefits. A lessons-learned session is a process of capturing and documenting the knowledge, experience, and feedback gained from a project, both positive and negative. A lessons- learned session helps to identify the strengths and weaknesses of the project management process, as well as the best practices and lessons for future projects. A lessons-learned session should be conducted at the end of each project phase or milestone, as well as at the end of the project.

However, even without a formal lessons-learned session, some learning may still occur informally or implicitly among the project team members or stakeholders.
* The projects 10% budget overrun was not reported to senior management: This is a significant finding, but not as significant as the lack of measurable benefits. A budget overrun is a situation where the actual cost of a project exceeds its planned or estimated cost. A budget overrun may indicate poor planning, estimation, or control of the project resources, or unexpected changes or risks that occurred during the project implementation. A budget overrun should be reported to senior management as soon as possible, along with the reasons for it and the corrective actions taken or proposed. However, a budget overrun may not necessarily affect the quality or value of the project deliverables or outcomes if they are still within acceptable standards or expectations.
* Monthly dashboards did not always contain deliverables: This is a significant finding, but not as significant as the lack of measurable benefits. A dashboard is a visual tool that displays key performance indicators (KPIs) or metrics related to a project's progress, status, or results. A dashboard helps to monitor and communicate the performance of a project to various stakeholders in a concise and clear manner. A dashboard should include deliverables as one of its components, along with other elements such as schedule, budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.
References: 1: The role & importance of the Post Implementation Review 2: What is Post-Implementation Review in Project Management?

NEW QUESTION: 203
□□ □ □□ □□□ □□ □□□ □□ □□□ □□□ □ IS □□□□ □□ □ □□□□ □□ □□□?
A. □□ □□□ □□ □□□□ □□□□ □□ □□□□.
B. □□ □□□□ □□ □□ □□□ □□□ □□□ □□□□.
C. □□ 1□ □□ □□ □□□ □□□□ □□□□□.
D. □□ □□ □□□ □□ □□□ □□□□□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)
The auditor should be most concerned about the security policy documents being available on a public domain website. This is because this exposes the organization's security posture and strategy to potential attackers, who can exploit the information to launch targeted attacks or bypass the security controls. The security policy documents should be classified as confidential and protected from unauthorized access or disclosure. The other options are less severe than exposing the security policy documents to the public, although they may also indicate some gaps or weaknesses in the security policy development, implementation, or maintenance process. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.31
* CISA Online Review Course, Domain 3, Module 1, Lesson 12

NEW QUESTION: 204
□□□□□ □□ □□□ □□□ □□□□□□ □□□□ □□ □□, □□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□□.
A. □□□ □□□□ □ □□□ □□□ □ □□□ □□□□□ □□□□□□□.
B. □□□□ □□□ □□□□ □□ □□□ □□□□□.
C. □□□□ □□□ □□□□ □□ □□□□ □□□□□□□.
D. □□□□ □□□□ □□ □□□ □ □□ □□□□□.
Answer: (SHOW ANSWER)
When a program release needs to be backed out of production, the changes introduced by that release must be removed from the source code to ensure the system returns to its prior state. This approach ensures that the source code reflects the stable version without the problematic changes.
References
* ISACA CISA Review Manual 27th Edition, Page 244-245 (Change Management)

NEW QUESTION: 205
□□□ □□ □□□□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□□.
A. □□ □□□□□ □□□ □□□ □□□ □.
B. □□□ □□□ □□□□ □.
C. □□□ □□□ □□□□ □□□ □□□ □□□□ □□.
D. □□□□ □□□ □□□ □□□ □□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 206
IS □□□□ □□□ □□□ □□□□□□□ □□□ □□□□ □□□□ □□□□ □□□ □ □□ □□ □□ □□□□ □□ □ □□□ □□ □□□□□. □□ □ □□ □□ □□□□ □ □□□ □□□□□□□□ □□ □□ □ □□□□□□?
A. □□□□□□ □□□ □□ □□□□□□ □□□□ □□
B. □□□□ □□□□ □□ □□□□ □□□□ □□ □□□ □□ □□ □□(SDLC) □ □□ □□
C. □□ □□(QA) □□□□ □□□ □□□ □□ □□□
D. □□□ □□□□□□ □□ □□ □□ □□□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 207
□□ □□□ □□□ □□ □□□ □□□□ IS □□□□ □□
A. □□□□□□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.
B. □□□□ □□ □ □□ □□□ □□□□□.
C. □□□□ □□ □□□□ □□□□□□.
D. □□□□ □□□ □□□□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)
The first step in assessing the controls within a newly implemented call center is to evaluate the operational risk associated with the call center. This will help the IS auditor to identify the potential threats, vulnerabilities, and impacts that could affect the call center's objectives, performance, and availability. The evaluation of operational risk will also provide a basis for determining the scope, objectives, and approach of the audit. The other options are possible audit procedures, but they are not the first step in the audit process. References: ISACA Frameworks: Blueprints for Success, CISA Review Manual (DigitalVersion)

NEW QUESTION: 208
□□ □ □□□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □ □□□□?
A. □□ □□ □□ □□□□□ □□□□□.
B. □□ □□ □□□ □□□□□□.
C. □□□□ □□ □□□ □□□□□.
D. □□ □□□□ □□ □□ □□□□□.
Answer: C (LEAVE A REPLY)
Automated version control systems are the best method to maintain an audit trail of changes made to the source code of a program. They automatically track and manage changes to the source code over time, allowing you to see what changes were made, when they were made, and who made them1. This provides a clear and detailed audit trail that can be invaluable for debugging, understanding the evolution of the code, and ensuring accountability23.

NEW QUESTION: 209
□□ □ □□□ □□□ □□ □ □□□ □□ □□□□□?
A. □□□□ □□□ □□□□.
B. □□□ □□□□□.
C. □□□ □□ □□□ □□□□ □□□□□.
D. □□□□ □□□□ □□ □□□□□.
Answer: (SHOW ANSWER)
A digital signature is a type of electronic signature that uses cryptographic techniques to provide authentication, integrity, and non-repudiation of digital documents. A digital signature is created by applying a mathematical function (called a hash function) to the document and then encrypting the result with the sender's private key. The encrypted hash, along with the sender's public key and other information, forms the digital signature. The receiver can verify the digital signature by decrypting it with the sender's public key and comparing the hash with the one computed from the document. If they match, it means that the document has not been altered and that it was signed by the owner of the private key.

Option D is correct because a digital signature is unique to the sender using it, as it depends on the sender's private key, which only the sender knows and controls. No one else can create a valid digital signature with the same private key, and no one can forge or modify a digital signature without being detected.
Option A is incorrect because a digital signature is not under control of the receiver, but rather under control of the sender. The receiver can only verify the digital signature, but cannot create or modify it.
Option B is incorrect because a digital signature is not capable of authorization, but rather capable of authentication. Authorization is the process of granting or denying access to resources based on predefined rules or policies. Authentication is the process of verifying the identity or legitimacy of a person or entity. A digital signature can authenticate the sender of a document, but it cannot authorize what actions the receiver can perform on the document.
Option C is incorrect because a digital signature does not dynamically validate modifications of data, but rather statically validates the integrity of data. A digital signature is based on a snapshot of the document at the time of signing, and any subsequent changes to the document will invalidate the digital signature. A digital signature does not monitor or update itself based on data modifications.
References:
CISA Online Review Course1, Module 5: Protection of Information Assets, Lesson 2: Encryption Basics, slide 13-14.
CISA Review Manual (Digital Version)2, Chapter 5: Protection of Information Assets, Section 5.2:
Encryption Basics, p. 273-274.
CISA Review Manual (Print Version), Chapter 5: Protection of Information Assets, Section 5.2: Encryption Basics, p. 273-274.
CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_712.
What Is a Digital Signature (and How Does it Work)1
What are digital signatures and certificates?2
Digital Signature Definition3
Examples and uses of electronic signatures4
What is an Electronic Signature?5

NEW QUESTION: 210
□□ □ IT □□□□□ □□□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□
B. □□ □□□□ □□
C. □□□□ □□ □□
D. □□□□ □□
Answer: (SHOW ANSWER)

The most critical factor for the effective implementation of IT governance is a supportive corporate culture. A supportive corporate culture is one that fosters collaboration, communication and commitment among all stakeholders involved in IT governance processes. A supportive corporate culture also promotes a shared vision, values and goals for IT governance across the organization. Strong risk management practices, internal auditor commitment or documented policies are important elements for IT governance implementation, but they are not sufficient without a supportive corporate culture.
References: ISACA, CISA Review Manual,
27th Edition, 2018, page 41

NEW QUESTION: 211
□□ □ □□□ □□□ □□□□ □□ □□□□ □□□□ □□ □□□□□?
A. □□□ □□ □□□□□.
B. □□□ □□□ □□□ □□□□ □□□□□.
C. □□□ □□□ □ □□□□.
D. □□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The best way to provide assurance of the integrity of a firewall log is to ensure that the log cannot be modified. A firewall log is a record of the traffic and events that occur at the firewall, which is a device or software that controls and filters the incoming and outgoing network traffic based on predefined rules and policies. The integrity of a firewall log means that the log is accurate, complete, consistent, and valid, and that it has not been altered, deleted, or corrupted by unauthorized or malicious parties. The IS auditor should verify that the firewall log has adequate controls to prevent or detect any modification of the log, such as encryption, hashing, digital signatures, write-once media, or tamper-evident seals. The other options are not as effective as ensuring that the log cannot be modified, because they either do not address the integrity of the log data, or they are monitoring or retention measures rather than preventive or detective controls. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 212
□□□ □□ IS □□□ □□□□ □□□□ □□ □□□ □□□□□?
A. □□□□ □□

B. □□□ □□ □□
C. □□ □□ □□
D. □□ □□ □□ □ □□
Answer: C (LEAVE A REPLY)
The primary basis for selecting which IS audits to perform in the coming year is the organizational risk assessment. An organizational risk assessment is a formal process for identifying, evaluating, and controlling risks that may affect the achievement of the organization'sgoals and objectives3. An organizational risk assessment can help IS auditors prioritize and plan their audit activities based on the level of risk exposure and impact of each area or process within the organization. An organizational risk assessment can also help IS auditors align their audit objectives and criteria with the organization's strategy and performance indicators.
Senior management's request, prior year's audit findings, and previous audit coverage and scope are also possible bases for selecting which IS audits to perform in the coming year, but not as primary as the organizational risk assessment. These factors are more secondary or supplementary sources of information that can help IS auditors refine or adjust their audit plan based on specific needs or issues identified by management or previous audits. However, thesefactors may not reflect the current or emerging risks that may affect the organization's operations or performance. References: ISACA CISA Review Manual 27th Edition, page 295

NEW QUESTION: 213
□□□ □□□ □□ □□ □□□ □□□□ IS □□□□ □□□ □□ □□ □□ □□□ □□ □□.
A. □□□ □□ □ □□□ □□□ □□□□ □□□□.
B. □□□ □□ □□□□ □□ □□□□ □□□ □□□□.
C. □ □□□ □□ □□□□ □□ □□□□□□□.
D. □□ □□□ □□□ □□□□□□□.
Answer: C (LEAVE A REPLY)
An IS auditor reviewing the threat assessment for a data center would be most concerned if the exercise was completed by local management, because this could introduce bias, conflict of interest, or lack of expertise in the assessment process. A threat assessment is a systematic method of identifying and evaluating the potential threats that could affect the availability, integrity, or confidentiality of the data center and its assets. A threat assessment should be conducted by an independent and qualified team that has the necessary skills, knowledge, and experience to perform a comprehensive and objective analysis of the data center's environment, vulnerabilities, and risks1.
The other options are not as concerning as option C for an IS auditor reviewing the threat assessment for a data center. Option A, some of the identified threats are unlikely to occur, is not a problem as long as the likelihood and impact of each threat are properly estimated and prioritized. A threat assessment should consider all possible scenarios, even if they

have a low probability of occurrence, to ensure that the data center is prepared for any eventuality2. Option B, all identified threats relate to external entities, is not a flaw as long as the assessment also considers internal threats, such as human errors, malicious insiders, or equipment failures. External threats are often more visible and severe than internal threats, but they are not the only source of risk for a data center3. Option D, neighboring organizations' operations have been included, is not a mistake as long as the assessment also focuses on the data center's own operations. Neighboring organizations' operations may have an impact on the data center's security and availability, especially if they share physical or network infrastructure or resources. A threat assessment should take into account the interdependencies and interactions between the data center and its external environment4.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* Data Center Threats and Vulnerabilities1
* Datacenter threat, vulnerability, and risk assessment2
* Data Centre Risk Assessment3

NEW QUESTION: 214
□□ □ □□□ □□□ □□ □□□□□ □□□□ □□ □ □□ □□□ □□□□□?
A. □□□ □□ □□□□□ □□ □□ □□□□□□ □□□□□.
B. □□□ □□ □□□□□ □□□□ □ □□□□ □□□□ □□□□□ □□□□□.
C. □□□ □□ □□□□□ □□ □□□ □□ □□□□.
D. □□ □□□ □□□□ □□□□ □□□ □□ □□□□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□ IS □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □ □□□□.
B. □□□ □□□□ □□□□ □□□□□ □□□ □ □□□□.
C. □□□□ □□□□ □ □ □□□□.
D. □□ □□□ IT □□□ □□□ □□□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)
The answer A is correct because the greatest concern for an IS auditor when a data owner assigns an incorrect classification level to data is that controls to adequately safeguard the data may not be applied. Data classification is the process of categorizing data assets based on their information sensitivity and business impact. Data classification helps organizations to identify, protect, and manage their data according to their value and risk.

Data owners are the individuals or entities who have the authority and responsibility to define, classify, and control the access and use of their data.
Data classification typically involves assigning labels or tags to data assets, such as public, internal, confidential, or restricted. These labels indicate the level of protection and handling required for the data.
Based on the data classification, organizations can implement appropriate controls to safeguard the data, such as encryption, access control lists, audit logs, backup policies, etc. These controls help to prevent unauthorized access, disclosure, modification, or loss of data, and to ensure compliance with relevant laws and regulations.
If a data owner assigns an incorrect classification level to data, it can result in either underprotection or overprotection of the data. Underprotection means that the data is classified at a lower level than it should be, which exposes it to higher risks of compromise or breach. For example, if a data owner classifies personal health information (PHI) as public instead of confidential, it may allow anyone to access or share the data without proper authorization or consent. This can violate the privacy rights of the data subjects and the compliance requirements of regulations such as HIPAA (Health Insurance Portability and Accountability Act). Overprotection means that the data is classified at a higher level than it should be, which limits its availability or usability. For example, if a data owner classifies marketing materials as restricted instead of public, it may prevent potential customers or partners from accessing or viewing the data. This can reduce the business value and opportunities of the data.
Therefore, an IS auditor should be concerned about the accuracy and consistency of data classification by data owners, as it affects the security and efficiency of data management. An IS auditor should review the policies and procedures for data classification, verify that the data owners have adequate knowledge and skills to classify their data, and test that the data classification labels match with the actual sensitivity and impact of the data.
References:
* Data Classification: What It Is and How to Implement It
* What Is Data Classification? - Definition, Levels & Examples ...
* Data Classification: A Guide for Data Security Leaders

NEW QUESTION: 216
□□□ □□ □□□□□ □□ □□□□□□ □□□ □□ CPU □□□ □□ □□□ □□□□ □□□□ □□□ □□□□□. □□ □ IS □□□□ IT □□□ □□ □□□□ □□ □□□□ □?
A. □□□ □□□ □□ □□□ □□□ □□□ □□□□ □ □□□□ □□□□□.
B. □□ □□ □ □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□□.
C. □□□□ □□□ □□ □ □□□ □□ □ □□ □□□ □□ □□□□□.
D. □□ □□ □□□ □□ □□□ □ □□ □□ □□□□ □□ □□□□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 217
□□ □ IS □□□□ □□ □ □□ □□ □□ □□□□ □□ □□ □□□□□?
A. □□□□ □□ □□ □□□ □□□□.
B. □□□□ □ □□ □□□ □□□ □□□□.
C. □□□ □□□ 3□ □□□□□□□.
D. □□□□ □□□ 15% □□□□□□.
Answer: A (LEAVE A REPLY)
A post-implementation review (PIR) is an assessment conducted at the end of a project cycle to determine if the project was indeed successful and to identify any existing flaws in the project1. One of the main objectives of a PIR is to evaluate the outcome and functional value of a project1. Therefore, an IS auditor should be most concerned with whether the system meets the intended requirements and delivers the expected benefits to the stakeholders. A system that does not have a maintenance plan is a major risk, as it may not be able to cope with changing needs, fix errors, or prevent security breaches. A maintenance plan is essential for ensuring the system's reliability, availability, and performance in the long term2.
The other options are less critical for a PIR, as they are more related to the project management aspects than the system quality aspects. The system may contain several minor defects that do not affect its functionality or usability, and these can be resolved in future updates. The system deployment may be delayed by three weeks due to unforeseen circumstances or dependencies, but this does not necessarily mean that the system is faulty or ineffective. The system may be over budget by 15% due to various factors such as scope creep, resource constraints, or market fluctuations, but this does not imply that the system is not valuable or beneficial.
References: 1: Post-Implementation Review Best Practices - MetaPM 2: What is Post-Implementation Review in Project Management?

NEW QUESTION: 218
□□□□ □□□□ □□□□ □□□□□ □□□□□ □□□□□ □□□ □□□□□. □□ □ □□ □□□ □□□□□ □□□?
A. □□□ □□□□ □□□□ □□□□□ □□□□□.
B. □□□ □□□□□ □ □□□□□
C. □□□ □□□□□□
D. □□□ □□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
An incident response team has been notified of a virus outbreak in a network subnet. The next step should be to focus on limiting the damage by containing the virus and preventing it from spreading further. This may involve isolating the affected systems, disconnecting them from the network, blocking malicious traffic or applying patches or antivirus updates. Verifying that the compromised systems are fully functional, documenting the incident and

removing and restoring the affected systems are possible steps that could be taken after limiting the damage. References:
* : [Incident Response Definition]
* : [Incident Response Process | ISACA]
* : [Virus Definition]

NEW QUESTION: 219
□□□ □□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □□□□□□□. □□ □ □ □□□□ □□ □ □□□□ □□ □□□□□?
A. □□□
B. □□□
C. □□ □□
D. □□ □□
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Monitoringcapacity utilizationsupportsavailabilityby ensuring thatresources remain functional and do not exceed operational limits.
* Option A (Incorrect):Integrityensures that data isaccurate and unaltered, but monitoring capacity thresholds primarily relates tosystem availability.
* Option B (Correct):Availabilityensures that systems remainaccessible and functional, and monitoring capacity utilization helpsprevent downtimeandservice disruptions.
* Option C (Incorrect):Confidentialityensures that data isprotected from unauthorized access, which is unrelated to capacity monitoring.
* Option D (Incorrect):Nonrepudiationensures that actions can betraced to specific individuals, but it does not relate tocapacity monitoring.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Coverscapacity planning and monitoring for system availability.

NEW QUESTION: 220
□□□□ □□□ □□ □□□ □□□□□ □□□□□□ □□□□ □□ □□ □□ □□ □□ □ □□ □ □□□□□?
A. □□□□ □□ □□
B. □□□ □□ □□
C. □□□ □□□ □□□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
The best audit procedure to determine whether a firewall is configured in compliance with the organization's security policy is reviewing the parameter settings. Parameter settings are values or options that define how a firewall operates and functions, such as rules, filters, ports, protocols, etc. By reviewing the parameter settings of a firewall, an IS auditor can verify whether they match with the organization's security policy, which is a document

that outlines the security objectives, requirements, and guidelines for an organization's information systems and resources. Reviewing the system log is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a system log records events or activities that occur on a firewall, such as connections, requests, responses, errors, alerts, etc., and may not indicate whether they comply with the organization's security policy. Interviewing the firewall administrator is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as a firewall administrator may not provide accurate or reliable information about the firewall configuration, and may have conflicts of interest or ulterior motives. Reviewing the actual procedures is a possible audit procedure to determine whether a firewall is configured in compliance with the organization's security policy, but it is not the best one, as actual procedures describe how a firewall is configured and maintained, such as installation, testing, updating, etc., and may not reflect whether they comply with the organization's security policy.

NEW QUESTION: 221
□□ □ IT □□□□□ □□ □□ □□□(QMS)□ □□□□□□ □□ □□ □□□□ □□□ □ □ □□ □□ □□□□□?
A. □□□□□□ □□ □□□ IT □□□ □□□
B. □□□ □□ □□□ □□□ □□□
C. IT □□□□□ □□ □□□ □□ □□(QA)□□ □□□
D. IT □□□ □□ □□□ □□□ □□ □□
Answer: A (LEAVE A REPLY)
Stakeholder satisfaction is a key indicator of the effectiveness of a QMS, as it reflects the extent to which the QMS meets the expectations and prioritiesof the customers and other interested parties. A high percentage of stakeholder satisfaction implies that the QMS is delivering consistent and reliable products or services that meet the quality standards and requirements.
References
ISACA CISA Review Manual, 27th Edition, page 253
The Four Main Components of A Quality Management System
The Road to Developing an Effective Quality Management System (QMS)

NEW QUESTION: 222
IS □□□□ IT □□□□ □□□ □□ □□ □□ □□□□ □□□ □□ □□ □□ □□□ □ □□□.
A. □□□ □□ □□□ □□□□□ □□□ □□□□□.
B. IT □□□ □□ □□ □□□ □□□□□ □□□□□.
C. IT □□□ □□□□ □□□□□.
D. IT □□□ □□□□□ □□□□□.

Answer: D (LEAVE A REPLY)
A balanced scorecard is a strategic planning framework that companies use to assign priority to their products, projects, and services; communicate about their targets or goals; and plan their routine activities1. The scorecard enables companies to monitor and measure the success of their strategies to determine how well they have performed. A balanced scorecard for IT management can help assess IT functions and processes by defining four perspectives: financial, customer, internal business process, and learning and growth2. These perspectives can help IT management align their IT objectives with the organization's vision and mission, identify and prioritize the key performance indicators (KPIs) for IT, and evaluate the effectiveness and efficiency of IT operations and services3.
References
1: Balanced Scorecard - Overview, Four Perspectives 2: The IT Balanced Scorecard (BSC) Explained - BMC Software 3: A BALANCED SCORECARD (BSC) FOR IT PERFORMANCE MANAGEMENT - SAS Support

NEW QUESTION: 223
□□ □ SQL □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□?
A. □ □□□□□□ □□□(WAF)
B. SQL □□ □□
C. □□ □□ □□□□
D. SQL □□ □□□ □□□
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:A Web Application Firewall (WAF) (A) is the best control to mitigate SQL injection attacks because it can detect and block malicious SQL queries before they reach the application. WAFs analyze incoming requests, filter SQL injection attempts, and provide an additional layer of security for web applications.
Other options:
* SQL server hardening (B) improves security but does not specifically address SQL injection.
* Patch management (C) is necessary but does not provide immediate protection against new SQL injection attacks.
* Physical controls (D) are unrelated to application-layer threats like SQL injection.
Reference: ISACA CISA Review Manual, Information Security

NEW QUESTION: 224
□□ □ □□□□ □□□(IM) □□□□ □□□ □□□ □□□ □□□□ □ □□ □□ □□ □□□ □□□□□?
A. IM□□ □□ □□ □□
B. □□ IM □□□ □□
C. □□□ IM □□□□ □□

D. IM □□□ □□□

Answer: (SHOW ANSWER)

Allowing only corporate IM solutions is the best control to mitigate the malware risk associated with an IM system, because it can prevent unauthorized or malicious IM applications from accessing the network and infecting the system with malware. Corporate IM solutions can also enforce security policies and standards, such as encryption, authentication, and logging, to protect the IM system from malware attacks. Blocking attachments in IM, blocking external IMtraffic, and encrypting IM traffic are also possible controls to mitigate the malware risk, but they are not as effective as allowing only corporate IM solutions. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.4

NEW QUESTION: 225

IS □□□□ IT □□□ □□□ □□□ □□□□□ □□□ □ □□□□ □ □□ □□□ □□ □□ □ □□□□□?

A. □□□□□(ROI)

B. □□ □□

C. □□□□ □□

D. □□□□□(TCO)

Answer: B (LEAVE A REPLY)

The answer B is correct because the most important thing for an IS auditor to review when determining whether IT investments are providing value to the business is the business strategy. The business strategy is the plan or direction that guides the organization's decisions and actions to achieve its goals and objectives.

The business strategy defines the organization's vision, mission, values, competitive advantage, target market, value proposition, and key performance indicators (KPIs).

IT investments are the expenditures or costs incurred by the organization to acquire, develop, maintain, or improve its IT assets, such as hardware, software, network, data, or services. IT investments can help the organization to support its business processes, operations, functions, and capabilities. IT investments can also help the organization to create or enhance its products, services, or solutions for its customers or stakeholders.

To determine whether IT investments are providing value to the business, an IS auditor needs to review how well the IT investments align with and contribute to the business strategy. Alignment means that the IT investments are consistent and compatible with the business strategy, and that they support and enable the achievement of the strategic goals and objectives. Contribution means that the IT investments are effective and efficient in delivering the expected outcomes and benefits for the business, and that they generate a positive return on investment (ROI) or value for money.

An IS auditor can use various methods or frameworks to review the alignment and contribution of IT investments to the business strategy, such as:

* Balanced scorecard: A balanced scorecard is a tool that measures and monitors the performance of an organization across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard can help an IS auditor to evaluate how well the IT investments support and improve each perspective of the organization's performance, and how they link to the organization's vision and strategy.
* Value chain analysis: A value chain analysis is a tool that identifies and analyzes the primary and support activities that add value to an organization's products or services. A value chain analysis can help an IS auditor to assess how well the IT investments enhance or optimize each activity of the value chain, and how they create or sustain a competitive advantage for the organization.
* Business case analysis: A business case analysis is a tool that evaluates the feasibility, viability, and desirability of a proposed project or initiative. A business case analysis can help an IS auditor to examine how well the IT investments address a business problem or opportunity, how they deliver the expected benefits and outcomes for the stakeholders, and how they compare with alternative options or solutions.
The other options are not as important as option B. Return on investment (ROI) (option A) is a metric that measures the profitability or efficiency of an investment by comparing its benefits or returns with its costs or expenses. ROI can help an IS auditor to quantify the value of IT investments for the business, but it does not capture all aspects of value, such as quality, satisfaction, or impact. ROI also depends on how well the IT investments align with the business strategy in the first place. Business cases (option C) are documents that justify and support a proposed project or initiative by describing its objectives, scope, benefits, costs, risks, and alternatives. Business cases can help an IS auditor to understand the rationale and expectations for IT investments, but they do not guarantee that the IT investments will actually deliver the desired value for the business. Business cases also need to be aligned with the business strategy to ensure their relevance and validity. Total cost of ownership (TCO) (option D) is a metric that measures the total costs incurred by an organization to acquire, operate, maintain, and dispose of an IT asset over its life cycle. TCO can help an IS auditor to estimate the financial impact of IT investments for the business, but it does not reflect the benefits or outcomes of IT investments, nor does it indicate how well the IT investments support or enable the business strategy.
References:
* IT Strategy: Aligning IT & Business Strategy
* How To Measure The Value Of Your Technology Investments
* IT Investment Management: A Framework for Assessing ... - GAO
* How To Align Your Technology Investments With Your Business Strategy

NEW QUESTION: 226
□□□ □□ □□(QA) □□□ □□ □□ □ IS □□□□ □□□□ □ □□ □□□□□?
A. □□ □□□□ □□□ □□□ □□□□□ □□
B. □□□ □□□ □□□ □□□□□ □□

C. □□ □□□ □□□□
D. □□□ □□□□ □□ □□□ □□
Answer: D (LEAVE A REPLY)
Implementing solutions to correct defects is a responsibility of the development function, not the quality assurance (QA) function. The QA function should ensure that the development process follows the established standards and methodologies, and that the defects are identified and reported. The QA function should not be involved in fixing the defects, as this would compromise its independence and objectivity. The other options are valid responsibilities of the QA function, and they should not raise concern for an IS auditor. References: CISA Review Manual (Digital Version) 1, page 300.

NEW QUESTION: 227
□□ □ □□□ □□ □□□ BYOD(Bring Your Own Device) □□□ □□□ □□ □□□ □ □□□ □ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□□□
B. □□□ □□ □□□□□ □□□□
C. □□□ □□ □□□ □□□□
D. □□□ □□ □□ □□□□
Answer: (SHOW ANSWER)
A mobile device awareness program would best enable an organization to address the security risks associated with a recently implemented bring your own device (BYOD) strategy. A mobile device awareness program is a set of activities that aim to educate and inform the employees about the benefits, challenges, and best practices of using their personal mobile devices for work purposes. A mobile device awareness program can help the organization to:
* Communicate the organization's policies and expectations regarding BYOD, such as which devices are allowed, what data can be accessed or stored, and what security measures are required.
* Raise the employees' awareness of the potential threats and vulnerabilities that affect their mobile devices, such as malware, phishing, data leakage, or device loss.
* Provide the employees with guidance and tips on how to protect their mobile devices and the organization's data, such as using strong passwords, encryption, antivirus software, remote wipe, or VPN.

* Encourage the employees to report any incidents or issues related to their mobile devices, such as suspicious messages, unauthorized access, or device damage.
A mobile device awareness program can help the organization to reduce the security risks associated with BYOD by enhancing the employees' knowledge, skills, and behavior in using their mobile devices securely and responsibly. A mobile device awareness program can also help the organization to comply with relevant regulations and standards that govern data privacy and security in the cloud1.
The other options are not as effective as a mobile device awareness program in enabling an organization to address the security risks associated with BYOD. Option A, mobile device tracking program, is a tool that allows the organization to monitor and locate the employees' mobile devices in case of loss or theft. However, this tool may not prevent or detect other types of security risks, such as malware infection or data breach.
Option B, mobile device upgrade program, is a process that ensures that the employees' mobile devices are running the latest versions of operating systems and applications. However, this process may not address other aspects of security, such as user behavior or data protection. Option C, mobile device testing program, is a method that verifies the functionality and compatibility of the employees' mobile devices with the organization's systems and networks. However, this method may not cover all the scenarios or factors that may affect the security of the mobile devices or the organization's data2.
References:
* Mobile Device Security Awareness Topics3
* Security Awareness Top Ten Topics - #8 Mobile Devices

NEW QUESTION: 228
IS □□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□ □□□□□ □□□□ □□□□. □ □□□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□ □ □□?
A. □□
B. □□
C. □□□□□
D. □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 229
IS □□ □□□□ □□□□ □□ □□□ □□□□□ □□□.
A. □□□□ □□□□ □ □□ □□□ □□ □□□ □□□□□.
B. □□□□ □□□ □□ □□□□ □□ □□.
C. □□□ □□□ □□□ □□□ □□.
D. □□□ □□ □□□□.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:

When outsourcingIS functions,independent audit provisionsensure thatcontractors meet security, compliance, and operational standards.
* Option A (Incorrect):Security procedures should be included but are subject tochangeandmay not be detailedin the contract.
* Option B (Correct):Independent audit rightsallow the organization toverifythat the vendor complies with security, operational, and regulatory requirements.
* Option C (Incorrect):Naming specific staff isimpracticaland not acore contractual requirement.
* Option D (Incorrect):Data transfer protocols are important, but they are atechnical detailrather than aprimary contract requirement.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Covers outsourcing, SLAs, and audit requirements.

NEW QUESTION: 230
□□ □□ □□ □ □□□ □□□ □□□□ □□ □ □□□ □□□□ □□ □□□□□?
A. □□□□ □□□□ □□ □□□ □□□□.
B. □□□□ □□□□ □□□ □ □□□□.
C. □□□□ □□ □□ □□□ □□□□ □□□□.
D. □□ □□□ □□ 1□ □□ □□□□□□ □□□□□.
Answer: (SHOW ANSWER)
The management decision that presents the greatest risk associated with data leakage is not providing security awareness training to staff. This is because staff are often the weakest link in the information security chain, and they may unintentionally or maliciously leak sensitive data through various channels, such as email, social media, cloud storage, or removable media. Security awareness training is essential to educate staff on the importance of protecting data, the policies and procedures for handling data, and the best practices for preventing and reporting data leakage incidents. Not requiring desktops to be encrypted, allowing staff to work remotely, and not updating security policies in the past year are also management decisions that may increase the risk of data leakage, but they are not as significant as not providing security awareness training to staff. Encryption, remote work, and security policies are technical or administrative controls that can be implemented or enforced by management, but they cannot fully prevent or mitigate human errors or malicious actions by staff. References: CISA Review Manual (Digital Version), [ISACA Privacy Principles and Program Management Guide]

NEW QUESTION: 231
□□ □□ □□ □ □□ □□ □□ □□□ □□□ □□ □□(DLP) □□□ □□□ □ □□□ □□□?
A. □□□□□(IoT)
B. □□□□ □□□
C. □□□□ □□□□

D. □□ □□□□ □□□(RPA)
Answer: (SHOW ANSWER)

NEW QUESTION: 232
□□□ □□ □□□ □□□(EUC)□ □□□ □□□ □□□□ IS □□□□□ □□ □ □□□ □ □□□ □□ □□□ □□□□□?
A. □ EUC □□□□□□□ □□□□ □□□□ □□□□□ □□□□ □□□□?
B. □□ □□□ □□ □□□□□ □□□□□.
C. EUC □□□□ □□ □□ □□ □□
D. EUC □□□□□□□ □□ □□□ □□□ □□□
Answer: (SHOW ANSWER)
The finding that should be of greatest concern to an IS auditor assessing the risk associated with end-user computing (EUC) in an organization is the lack of defined criteria for EUC applications. EUC applications are applications that are developed and maintained by end-users, rather than by IT professionals, to support their business functions and processes. Examples of EUC applications include spreadsheets, databases, reports, and scripts. The lack of defined criteria for EUC applications means that the organization does not have clear and consistent standards or guidelines to identify, classify, and manage EUC applications. This can lead to various risks, such as:
* Inaccurate or unreliable data and results from EUC applications that are not validated, verified, or tested
* Unauthorized or inappropriate access or use of EUC applications that are not secured, controlled, or monitored
* Inconsistent or incompatible data and results from EUC applications that are not integrated, documented, or updated
* Loss or corruption of data and results from EUC applications that are not backed up, recovered, or archived Therefore, the IS auditor should be most concerned about the lack of defined criteria for EUC applications, as it can affect the quality, integrity, and availability of the EUC applications and the data they produce.
Insufficient processes to track ownership of each EUC application is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. The ownership of an EUC application refers to the person or group who is responsible for creating, maintaining, and using the EUC application. Insufficient processes to track ownership of each EUC application means that the organization does not have adequate mechanisms or records to identify and communicate who owns each EUC application. This can lead to risks, such as:
* Lack of accountability or ownership for the quality and accuracy of the EUC application and its data
* Lack of support or maintenance for the EUC application when the owner leaves or changes roles

* Lack of awareness or training for the users of the EUC application on its purpose and functionality However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
Insufficient processes to test for version control is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Version control is a process that tracks and manages the changes made to an EUC application over time. Insufficient processes to test for version control means that the organization does not have adequate procedures or tools to ensure that the changes made to an EUC application are authorized, documented, and tested. This can lead to risks, such as:
* Errors or inconsistencies in the data and results from different versions of the EUC application
* Conflicts or confusion among the users of the EUC application on which version is current or correct
* Loss or overwrite of data and results from previous versions of the EUC application However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
Lack of awareness training for EUC users is a finding that should be of concern to an IS auditor assessing the risk associated with EUC in an organization, but it is not the greatest concern. Awareness training for EUC users is a process that educates and informs the users of the EUC applications on their roles, responsibilities, and risks. Lack of awareness training for EUC users means that the organization does not have adequate programs or materials to raise the knowledge and skills of the users on how to use and manage the EUC applications effectively and securely. This can lead to risks, such as:
* Misuse or abuse of the EUC applications by users who are not aware of their impact or implications
* Non-compliance or violation of policies or regulations by users who are not aware of their requirements or expectations
* Dissatisfaction or frustration among users who are not aware of their benefits or limitations However, these risks are less severe than those caused by the lack of defined criteria for EUC applications.
References:
* End-user computing - Wikipedia 1
* How to Manage the Risks Associated with End User Computing 2
* Managing end user computing risks - KPMG UK 3

NEW QUESTION: 233
□□□□□ □□ □□□□ □□□□□□□ □□ □□ □□□□ □□□□□. □□□ □□ □ □□ □□□ □□ □□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□□ □□ □□□ □□ □□□ □□ □□□□□ □□□□□.
B. □□□□ □□□ □□ □□□ □□□□□.

C. □□ □□ □ □□□ □□ □□ □□

D. □□□□□ □□ □□ □□□ □□ □□ □□□ □□□□□ □□□□□.

Answer: (SHOW ANSWER)

A vendor requires privileged access to a key business application. The best recommendation to reduce the risk of data leakage is to implement real-time activity monitoring for privileged roles. This is because real-time activity monitoring can provide visibility and accountability for the actions performed by the vendor with privileged access, such as creating, modifying, deleting, or copying data. Real-time activity monitoring can also enable timely detection and response to any unauthorized or suspicious activities that may indicate data leakage. Including the right-to-audit in the vendor contract is a good practice, but it may not be sufficient to prevent or detect data leakage in a timely manner, as audits are usually performed periodically or on-demand.

Performing a review of privileged roles and responsibilities is also a good practice, but it may not address the specific risk of data leakage by the vendor with privileged access. Requiring the vendor to implement job rotation for privileged roles may reduce the risk of collusion or fraud, but it may not prevent or detect data leakage by any individual with privileged access. References: CISA Review Manual (Digital Version),
[ISACA Privacy Principles and Program Management Guide]

NEW QUESTION: 234

□□ □□ □□□ □□ □□□□ □□ □□(AI) □□□□□ □□□□ □□□□□ □□□ □ IS □□□□ AI□ □□□ □□□ □□□ □□ □□ □□□□ □□□.

A. □□ □□

B. □□□□□□ □□□□(EA)

C. □□ □□ □□□□

D. □□ □□ □□

Answer: (SHOW ANSWER)

The auditor should be most concerned with the impact AI will have on enterprise architecture (EA) when reviewing a project to replace multiple manual data entry systems with an AI system. EA is a comprehensive framework that defines the structure, components, relationships, and principles of an organization's IT environment. EA can help to align the IT strategy with the business strategy and ensure the coherence, consistency, and integration of the IT systems and services. Replacing manual data entry systems with an AI system may have significant implications for the EA, such as changing the business processes, data flows, security requirements, performance standards, or governance models. The auditor should assess whether the project has considered the impact of AI on EA and whether the EA has been updated accordingly. References:

* CISA Review Manual (Digital Version), Chapter 1, Section 1.41
* CISA Online Review Course, Domain 5, Module 1, Lesson 22

NEW QUESTION: 235

□□ □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□ □□ □□ □□□□ □□□ □□□. □□ □ □□ □ □□□ □□ □□□ □□□□□?

A. □□ □□□ □□□ □□□□□ □□□□ □ □□□□.

B. □□ □□ □□□□ □□□□□ □□□ □□ □□□□□□.

C. □□□ □□□□ □□ □□ □□□□ □□□ □□ □□ □□□ □ □□□□.

D. □□□ □□□□□ □□ □□□□ □□□□□.

Answer: A (LEAVE A REPLY)

A distributed security administration system is a system that allows different administrators to manage the security of different parts of the network or organization. This can provide more flexibility, scalability, and efficiency than a centralized system, where one administrator is responsible for the entire security. However, a distributed security administration system also presents some potential challenges and risks, such as:

* Inconsistency and conflict among different security policies and standards
* Lack of coordination and communication among different administrators
* Difficulty in monitoring and auditing the overall security status and performance
* Increased complexity and cost of security management and maintenance

Therefore, the greatest potential concern for implementing a distributed security administration system is that the security procedures may be inadequate to support the change. Security procedures are the rules and guidelines that define how security is implemented and enforced in an organization. They include policies, standards, processes, roles, responsibilities, controls, and metrics. Security procedures should be aligned with the business objectives, risks, and requirements of the organization, as well as the best practices and regulations in the industry. Security procedures should also be reviewed and updated regularly to reflect the changes in the environment, technology, and threats.

If the security procedures are not adequate to support the change from a centralized to a distributed security administration system, the organization may face increased security risks, such as unauthorized access, data breaches, compliance violations, reputation damage, and financial losses. Therefore, it is essential to ensure that the security procedures are revised and adapted to suit the new system, and that they are communicated and enforced effectively across the organization.

References:

* 1: Security in Distributed System - GeeksforGeeks
* 2: Distributed System Security Architecture - Wikipedia
* 3: Distributed Systems Security: Issues, Processes and Solutions

NEW QUESTION: 236

IT □□□□ □□□□□□ □□□□□ □□□ □□□□ □□□ □□□□ □□□.

A. □□□□ IT □□□ □□□□□.

B. □□ IT □□□□□□ □□ □□□□□.

C. IT □□ □□□□ □□□□□.

D. IT □□□ □□□□□.

Answer: (SHOW ANSWER)

IT governance is a framework that defines the roles, responsibilities, and processes for aligning IT strategy with business strategy. The board of directors of an organization is ultimately accountable for IT governance and has the authority to approve the IT strategy. The board of directors does not need to address technical IT issues, be informed of all IT initiatives, or have an IT strategy committee, as these tasks can be delegated to other stakeholders or committees within the organization.

NEW QUESTION: 237

□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□?

A. □□ □□□□ □□ □□□□ □ □□□□ □□□□□.

B. □□□ □□□□ □□□ □□□□ □□□ □□□□□ □□□□□.

C. □□ □□□□ □□□□ □□□ □□

D. □□ □□□□ □□□ □□□□ □□□□□

Answer: D (LEAVE A REPLY)

The primary purpose of performing a parallel run of a new system is to validate the new system against its predecessor. A parallel run is a strategy for system changeover where a new system slowly assumes the roles of the older system while both systems operate simultaneously. This allows for comparison of the results and outputs of both systems to ensure that the new system is working correctly and reliably. A parallel run can also help identify and resolve any errors, discrepancies, or inconsistencies in the new system before the old system is discontinued.

The other options are not the primary purpose of performing a parallel run of a new system. A. To train the end users and supporting staff on the new system. Training is an important part of system implementation, but it is not the main reason for doing a parallel run. Training can be done before, during, or after the parallel run, depending on the needs and preferences of the organization. B. To verify the new system provides required business functionality. Verifying the business functionality of the new system is part of user acceptance testing (UAT), which is a formal and structured process of testing whether the new system meets the specifications and expectations of the users and stakeholders. UAT is usually done before the parallel run, as a prerequisite for system changeover. C. To reduce the need for additional testing. Reducing the need for additional testing is not the primary purpose of performing a parallel run, but rather a possible benefit or outcome of doing so. A parallel run can help ensure that the new system is thoroughly tested and validated in a real-worldenvironment, which may reduce the likelihood of encountering major issues or defects later on.

However, additional testing may still be needed after the parallel run, depending on the feedback and evaluation of the users and stakeholders.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471

* IS

NEW QUESTION: 238
□□ □□ □□ □□ IS □□□□ □□ □□ □□ □□ □□ □□□ □□□ □□□□□□ □ □□□□□. □□ □ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□□□ □□□□□ □□□□□.
B. □□ □□ □□□ □□□□□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□ □□□□□ □□□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The IS auditor's most important course of action after finding that several similar incidents were logged during the audit period is to determine if a root cause analysis was conducted. A root cause analysis is a systematic process that identifies the underlying causes of system failures or incidents. A root cause analysis can help to prevent recurrence of similar incidents, improve system performance and reliability, and enhance incident management processes. The IS auditor should evaluate whether a root cause analysis was performed for each incident, whether it was timely and thorough, and whether it resulted in effective corrective actions.

NEW QUESTION: 239
□□ □ □□□ □□ □□□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□□ □□□□ □□ □□□ □□ □□
B. □□□ □□ □□□ □□ □□
C. □□□□□ □□□□□ □□□□ □□ □□ □□
D. □□ □□□ □□ □□ □□ □ □□□□
Answer: B (LEAVE A REPLY)
The best way to verify the effectiveness of a data restoration process is to perform periodic complete data restorations. This is the process of transferring backup data to the primary system or data center and verifying that the restored data is accurate, complete, and functional. By performing periodic complete data restorations, the auditee can test the reliability and validity of the backup data, the functionality and performance of the restoration tools and procedures, and the compatibility and integrity of the restored data with the primary system. This will also help identify and resolve any issues or errors that may occur during the restoration process, such as corrupted or missing files, incompatible formats, or configuration problems.
Performing periodic reviews of physical access to backup media (option A) is not the best way to verify the effectiveness of a data restoration process, as it only ensures the security and availability of the backup media, not the quality or usability of the backup data. Physical access reviews are important for preventing unauthorized access, theft, damage, or loss of backup media, but they do not test the actual restoration process or verify that the backup data can be successfully restored.

Validating offline backups using software utilities (option C) is also not the best way to verify the effectiveness of a data restoration process, as it only checks the integrity and consistency of the backup data, not the functionality or compatibility of the restored data. Software utilities can help detect and correct any errors or inconsistencies in the backup data, such as checksum errors, duplicate files, or incomplete backups, but they do not test the actual restoration process or verify that the restored data can work with the primary system.
Reviewing and updating data restoration policies annually (option D) is also not the best way to verify the effectiveness of a data restoration process, as it only ensures that the policies are current and relevant, not that they are implemented and followed. Data restoration policies are important for defining roles and responsibilities, objectives and scope, standards and procedures, and metrics and reporting for the restoration process, but they do not test the actual restoration process or verify that it meets the expected outcomes.
Therefore, option B is the correct answer.
References:
* Whatis backup and disaster recovery? | IBM
* Backup and Recovery of Data: The Essential Guide | Veritas
* Database Backup and Recovery Best Practices - ISACA

NEW QUESTION: 240
□□□ □□□□ □□□□ □□□□ □□□ □□ □ □□ □□□ □□□ □□ □□ □□□ □ □□ □□□ □□ □ □□□□□?
A. □□□□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
B. □□□□ □□ □□ □□ □□□ □□ □□□.
C. □□□□ □□□ □□□ □□ □□ □□ □□□ □□□ □□□ □□□.
D. □□□□ □□ □□□□ □□□□ □□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 241
□□□ □□ □□(ACL)□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□□□ □ □□□□. □ □□□ □□□ □□□□. (CISA □□ - □□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□ □□/□□□ □□□□□.)
A. □□ □□□□ □□□□ □□□□□.
B. Telnet□ □□ □□□□ □□□□ □□□ □ □□□□.
C. □□□ □□□□ □□□ □□□ □□□ □□□.
D. □□□ □□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)
The use of access control lists (ACLs) is the most effective method to mitigate security risk for routers because they can limit Telnet and traffic from the open Internet. Telnet is a protocol that allows remote access to a device, which can pose a security threat if not

properly controlled. Traffic from the open Internet can also contain malicious packets that can harm the network or the router itself. ACLs act as filters that can block or allow specific types of traffic based on predefined criteria, such as source and destination addresses, protocols, ports, and flags. By using ACLs, routers can prevent unauthorized access and reduce the exposure to potential attacks.
References:
* Protecting Your Core: Infrastructure Protection Access Control Lists
* Definition, purposes, benefits, and functions of ACL
* CISA Review Manual 27th Edition, page 336

NEW QUESTION: 242
□□□ □□□ □, □□□□ □□ □□□ □□□□□ □ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□
D. □□□□□□
Answer: (SHOW ANSWER)
Following a breach, the maximum amount of time before customers must be notified that their personal information may have been compromised depends on the industry regulations that apply to the organization.
Different industries and jurisdictions may have different legal and regulatory requirements for breach notification, such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, or the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada. Industry standards, incident response plans, and information security policies are not as authoritative as industry regulations in determining the breach notification time frame. References: CISA Review Manual (Digital Version), [ISACA Privacy Principles and Program Management Guide]

NEW QUESTION: 243
IS □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
□□□□ □□□ □□□ □□□?

A. □□□□□ □□□ □□□□ □□□ □□ □□
B. □□ □□□ □□□ □□□ □□□□ □□
□□□□□
C. □□□□ □□□ □□□ □ □□□□ □□ □□
□□□□
D. □□□ □□□ □□□ □ □ □□□□ □□□□ □□
Answer: C (LEAVE A REPLY)
The most important thing for an IS auditor to look for in a project feasibility study is an assessment of whether the expected benefits can be achieved. A project feasibility study is a preliminary analysis that evaluates the viability and suitability of a proposed project based on various criteria, such as technical, economic, legal, operational, and social factors. The expected benefits are the positive outcomes and value that the project aims to deliver to the organization and its stakeholders. The IS auditor should verify whether the project feasibility study has clearly defined and quantified the expected benefits, and whether it has assessed the likelihood and feasibility of achieving them within the project scope, budget, schedule, and quality parameters. The other options are also important for an IS auditor to look for in a project feasibility study, but not as important as an assessment of whether the expected benefits can be achieved, because they either focus on specific aspects of the project rather than the overall value proposition, or they assume that the project will be implemented rather than evaluating its viability. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.1

NEW QUESTION: 244
□□□□ □□□ □□ □□ □□ □□□□□□ □ □□ □□□ □□ □ □□□□□?
A. □□□□□ □□□ □□ □□□□ □□ □□ □□□ □□□□.
B. □□ □□□□ □□ □□ □□□ □□□□.
C. □□□ □□□ □□□□ □□□□□.
D. □3□□ □□□□ □□□ □□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
The first step in the incident response process for a suspected breach is to research the validity of the alerted breach. An incident response process is a set of procedures that defines how to handle security incidents in a timely and effective manner. The first step in this process is to research the validity of the alerted breach, which means to verify whether the alert is genuine or false positive, to determine the scope and impact of the incident, and to gather relevant information for further analysis and action. Informing potentially affected customers of the security breach, notifying business management of the security breach, and engaging a third party to independently evaluate the alerted breach are also steps in the incident response process, but they are not the first step. References:
* CISA Review Manual, 27th Edition, page 4251
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 245
IS □□□□ □□□□ □□ □□□ □ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□. □□ □ □□□□□ □□ □ □□□□ □□□□□?
A. □ □□□ □□ □□□□ □□□ □□□□□ □□□ □□□□ □□□□□□□□.
B. □□□ □□□□ □ □□□ □□□ □□□ □□□ □ □□ □□□□ □□□□□.
C. □□□□ □□□□□ □□□ □□□□ □□□ □□□□□□.
D. □□ □□□□□ □□□ □□□□ □□□ □□□□□ □ □□□□ □□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 246
□□□□ □□ □□□□□□ □□□□□ □□□□□ □□□□□ □□□□□ □□ □□□□ □□□ □ □□ □□□?
A. □□□□ □□□□□(DMZ)□ □□□□ □□□.
B. □□ □□□ □□ □□□ □□□□ □□□.
C. □□ □□ □□□ □□□□ □□ □□□□□ □□□.
D. □□□□ □□ □□□□ □□□□□ □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 247
□□ □ IT □□□ □□□ □□□ □□□ □□□□□ □□ □□ □ □□□□ □□ □□□□ □?
A. IT □□□ □□ □□□□ □□ □□□□□ □□□□□.
B. □□ □□□ □□□□□□□□(CIO)□□ □□□□□.
C. □□□□ □□ □□□□ IT □□ □□□ □□□□□.
D. □□□□□□□(CIO)□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Business stakeholders being involved in approving the IT strategy best demonstrates that IT strategy is aligned with organizational goals and objectives. IT strategy is a plan that defines how IT resources and capabilities will support and enable the achievement of business goals and objectives. Business stakeholders are the individuals or groups who have an interest or influence in the organization's activities and outcomes.
By involving business stakeholders in approving the IT strategy, the organization can ensure that the IT strategy reflects and supports the business needs, expectations, and priorities. The other options do not necessarily indicate that IT strategy is aligned with organizational goals and objectives, as they do not involve the participation or feedback of business stakeholders. References: CISA Review Manual, 27th Edition, page
97

NEW QUESTION: 248
□□□ □□□□ □□ □□ □□□ □□□□□ □□□□ □□□□ □□ □□ □ □□ □□ □□□□ □□□?

A. □□□□□□ □□□□ □□□ □ □□ □□ □□□ □□
B. □□ □□□ □□ □□ □□ □□
C. □□□□ □□ □□□ □□□ □□□
D. □□ □□ □□ □□
Answer: D (LEAVE A REPLY)
Providing security certification for a new system should include an evaluation of the configuration management practices prior to the system's implementation. Configuration management is a process that ensures that the system's components are identified, controlled, and tracked throughout the system's lifecycle.
Configuration management helps to maintain the security and integrity of the system by preventing unauthorized or unintended changes. End-user authorization to use the system in production is not part of security certification, but rather a post-implementation activity that grants access rights to authorized users.
External audit sign-off on financial controls is not part of security certification, but rather a verification activity that ensures that the system complies with financial reporting standards. Testing of the system within the production environment is not part of securitycertification, but rather a validation activity that ensures that the system meets the functional and performance requirements. References:
* CISA Review Manual, 27th Edition, pages 449-4501
* CISA Review Questions, Answers& Explanations Database, Question ID: 2572

NEW QUESTION: 249
□□□ □□ □□□ □□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □ □□□. □□ □ □□ □□□ □ □□□ □□□□ □ □□ □□□□□?
A. □□□ □□□ □□□□□ □□□.
B. □□ □□ □□□ □□□ □□ □□□ □.
C. □□ □□□ □□ □□□ □□ □.
D. □□□ □□□ □□□□□ □□
Answer: A (LEAVE A REPLY)
The best metric to assure compliance with the policy of providing security awareness training to all new employees is the percentage of new hires that have completed the training, as this directly measures the extent to which the policy is implemented and enforced. The number of new hires who have violated enterprise security policies, the number of reported incidents by new hires, and the percentage of new hires who report incidents are not directly related to the policy, as they may depend on other factors such as the nature and frequency of threats, the effectiveness of security controls, and the reporting culture of the organization. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.7

NEW QUESTION: 250

□□□ □□□□ □□ □□□ □□□□□ □□□ □□□□ □□□ □□ □□□□ □□□□.
IS □□□□ □□□ □□□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □□ □ □ □ □□□□?

A. □□□ □□ □□ □□(CAAT)

B. □□□ □□□

C. □□□ □□□

D. □□□□ □□

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

To efficiently detectduplicate payments,data analyticsand automated checks are required due to thehigh volume of transactions.

* Option A (Correct):Computer-Assisted Audit Techniques (CAATs)allow auditors toautomatically scan large datasetsfor duplicate payments based oninvoice numbers, vendor names, and payment amounts.
* Option B (Incorrect):Stratified samplinggroups data into categories, which helps in analysis but does not directly detect duplicates.
* Option C (Incorrect):Statistical samplingis useful forextrapolating results, but it doesnot systematically findduplicate transactions.
* Option D (Incorrect):Process walk-throughsreview procedures but donot analyze transactions at scale.

Reference:ISACA CISA Review Manual -Domain 2: Governance and Management of IT-Covers CAATs, data analytics, and fraud detection techniques.

NEW QUESTION: 251

□□□□ □□□□, □□□ □□ □□□□ □□□ □□□ □□ □ □□□ □□ □ □□□□ □?

A. □□ □□ □□(BIA)□ □□□□ □□□□□.

B. □□ □□□□ □□□□ □□□□ □□□□ □□□□□.

C. □□□ □□□□ □□□□ □□□ □□□□.

D. □□□□ □□□□ □□□ □□ □□□(UAT)□ □□□□ □□□□□.

Answer: A (LEAVE A REPLY)

Resilience is the ability of an organization to continue to operate effectively during or after a disruptive event. A business impact analysis (BIA) is a key process to identify the critical systems and processes that support the organization's objectives and determine the impact of their disruption. Without a BIA, the organization may not be able to prioritize the recovery of the most important systems and processes, which poses the greatest risk to its resilience. The other options are not as significant as a BIA, as they relate to data quality, system monitoring, and user acceptance testing, which are important but not essential for resilience. References: CISA Review Manual (Digital Version), Domain 4: Information Systems Operations and Business Resilience, Section 4.2 Business Continuity Planning1

NEW QUESTION: 252
□□□ □□ □□□ □□□□ □ □□ □□ □□ □□□ □□ □□□ □□ □ □□□□□ □ □□?
A. □□ □□□ □□
B. □□ □□ □□□□□ □□
C. □□ □□ □□(ERM) □□
D. □□ □□ □□□□□ □□
Answer: C (LEAVE A REPLY)
The primary role of an internal audit function in the management of identified business risks is to validate the enterprise risk management (ERM) process and provide assurance on its effectiveness. The internal audit function should evaluate whether the ERM process is aligned with the organization's objectives, strategies, policies and culture, and whether it covers all relevant risks and controls. The internal audit function should also assess whether the ERM process is operating as designed and producing reliable and timely information for decision making. The other options are not the primary role of an internal audit function, but rather the responsibilities of senior management, board of directors or risk owners. References:
* ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.41
* ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 12072

NEW QUESTION: 253
□ □□□□ □□□ □□□ □□□ □□□□ □□ □ □□ □□□ IS □□□□ □□□□□ □. □□□ □ □ □□ IT □□ □□□ □□□ □□, □ □□ □□□ □□□ □□□ □□□□. □□ □ IS □□ □□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□□ □□ □□□ □□ □□□□□ □□□.
B. □□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□.
C. □□ □ □ □□□□ □□□□□ □□□□ □□□□□ □□□ □□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□ □□□□ □ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The IS audit standard for proficiency states that the IS auditor must have the knowledge, skills and experience needed to perform the audit work. This implies that the IS auditor must be competent in both the technical and business aspects of the audit subject matter. Therefore, team member assignments must be based on individual competencies, so that each auditor can perform the tasks that match their qualifications and expertise. This will also ensure that the audit objectives are met and the audit quality is maintained.
Option B is incorrect because technical co-sourcing is not a requirement to meet the IS audit standard for proficiency. Co-sourcing is an option that may be used when the internal audit function lacks the necessary resources or skills to perform the audit work. However, co-sourcing does not guarantee that the new staff will acquire the proficiency needed for

the audit. Moreover, co-sourcing may introduce additional risks and challenges, such as confidentiality, independence, communication and coordination issues.
Option C is incorrect because having a globally recognized audit certification does not necessarily mean that the standard for proficiency is met. A certification is an indication of the auditor's knowledge and competence in a specific domain, but it does not cover all aspects of IS auditing. The auditor must also have relevant experience and continuous learning to maintain and enhance their proficiency. Furthermore, having one certified member does not ensure that the other members are also proficient.
Option D is incorrect because having a supervisor review the new auditors' work is not sufficient to meet the IS audit standard for proficiency. A supervisor review is a quality assurance measure that helps to ensure that the audit work is performed in accordance with the standards and policies. However, a supervisor review does not substitute for the proficiency of the auditors who perform the work. The auditors must still have the necessary knowledge, skills and experience to conduct the audit tasks effectively and efficiently.
References:
CISA Online Review Course1, Module 1: The Process of Auditing Information Systems, Lesson 2:
Mandatory Guidance, slide 8-9.
CISA Review Manual (Digital Version)2, Chapter 1: The Process of Auditing Information Systems, Section
1.3: Mandatory Guidance, p. 24-25.
CISA Review Manual (Print Version), Chapter 1: The Process of Auditing Information Systems, Section 1.3:
Mandatory Guidance, p. 24-25.
CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_711.

NEW QUESTION: 254
□□ □ □□ □□ □□□□□ □□□ □□ □ □□□□□ □□ □□□□□?
A. □□ □□ □□ □□□ □□ □□ □□ □□
B. □□ □□□ □□□□ □□ □□□□, □□ □ □□ □□(GRC) □□ □□
C. □□ □□ □□ □□ □□ □□ □ □□
D. □□□ □□□□ □□ □□ □□ □□□□
Answer: (SHOW ANSWER)
Assessing and tracking all compliance audit findings is the best way to support the effectiveness of a compliance program. This allows an organization to identify areas of non-compliance, take corrective action, and monitor improvements over time12. While implementing an awareness plan, using a governance, risk, and compliance (GRC) tool, and monitoring applicable regulations can contribute to a compliance program, they do not provide the same level of continuous improvement and effectiveness as assessing and tracking audit findings.

NEW QUESTION: 255
□□ □ □□□ □□□□□□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□
B. □□ □□ □□(RTO)□ □□□□ □□
C. □ □□ □□□ □□□□ □□ □□
D. □□□ □□□□ □□□□□□
Answer: D (LEAVE A REPLY)
Clustering is a technique that groups multiple servers or nodes together to act as one system, providing high availability, scalability, and load balancing for applications or services. Clustering can improve system resiliency, which is the ability of a system to withstand or recover from failures or disruptions without compromising its functionality or performance. Clustering can achieve this by providing redundancy and fault tolerance for critical components or processes, enabling automatic failover and recovery in case of node failures, distributing workload among multiple nodes to avoid overloading or bottlenecks, and allowing dynamic addition or removal of nodes to meet changing demand or capacity needs. Clustering may also decrease system response time by improving performance and efficiency through load balancing and parallel processing, but this is not its primary purpose. Clustering may facilitate faster backups by enabling concurrent backup operations across multiple nodes, but this is not its main benefit. Clustering may improve the recovery time objective (RTO), which is the maximum acceptable time for restoring a system or service after a disruption, by reducing the downtime and data loss caused by failures, but this is not the best reason for using clustering, as there may be other factors that affect the RTO, such as backup frequency, recovery procedures, and testing methods.

NEW QUESTION: 256
□□ □ □□ □□ □□(BIA)□ □□□ □ □□□□ □□□□ □□□□□?
A. □□ □□□ □□ □□□ □□□ □□ □□
B. □□ □□□ □□□□ □ □□ □□□□□ □□
C. □□ □□ □□
D. □□□□□ □□□ □□□□
Answer: D (LEAVE A REPLY)
The expected costs for recovering the business would be used when performing a business impact analysis (BIA). A BIA is a process of identifying and evaluating the potential effects of disruptions to critical business functions or processes. A BIA helps to determine the recovery priorities, strategies, and resources needed to resume normal operations after a disruption. One of the key outputs of a BIA is an estimate of the financial losses or costs associated with different types of disruptions, such as lost revenue, increased expenses, contractual penalties, or regulatory fines.

NEW QUESTION: 257
□□ □ □□□□□ □□□□ □□□□ □□ □□□ □□ □□□□□?
A. □□□ □□□
B. □□□ □□□
C. □□ □□ □□□
D. □□ □□ □□ □□□
Answer: B (LEAVE A REPLY)
Substantive testing is the most important type of testing during software license audits, as it provides evidence of the accuracy and completeness of the software inventory and licensing records. Substantive testing involves examiningtransactions, balances, and other data to verify their validity, existence, accuracy, and valuation. Compliance testing, on the other hand, is more focused on assessing the adequacy and effectiveness of internal controls over software licensing, such as policies, procedures,and monitoring mechanisms. Compliance testing alone cannot provide sufficient assurance that the software license audit objectives are met, as itdoes notverify the actual software usage and compliance status. Judgmental sampling and stop-or-go sampling are methods of selecting samples for testing, not types of testing themselves. *References:
According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 1206 Testing, "The IS audit and assurance professional should perform sufficient testing to obtain sufficient appropriate evidence to support conclusions reached." 1 The section also defines substantive testing as "testing performed to obtain audit evidence to detect material misstatements in transactions orbalances" and compliance testing as "testing performed to obtain audit evidence on theoperating effectiveness of controls." 1 According to the ISACA IT Audit and Assurance Guideline G15 Software License Management, "The objective of a software license auditis to provide management with an independent assessment relating to compliance with software license agreements." 2 The guideline also states that "substantive tests should be performed on a sample basis to verify that all software installed on devices within scope has been appropriately licensed." 2

NEW QUESTION: 258
□□□ □□ □□□□ □□□□ □□ □ □□□ □□□ □□□ □□ □□□□ □□□ □□ □ □□□□□.
A. □□□ IP □□□ □□ □□□□ □□□□□□.

B. □□ □□□ □□ □□ □□ □□□ □□□□□.
C. □□ □□□□ □□ □□□ □□□□□.
D. □□□ □□□ □□□□□ □□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
A web proxy server for corporate connections to external resources reduces organizational risk by anonymizing users through changed IP addresses. A web proxy server is an intermediarybetween the web and client devices, that can provide proxy services to a client or a group of clients1. One of the main benefits of using a web proxy server is that it allows users to change their IP address andlocation, circumventing geoblocking and hiding their identity from the target website2.
Anonymizing internal IP addresses is important for online security, as it helps protect the organization from several threats. If an attacker controls a server that employees connect to, the outgoing IP address of the organization's router is logged on the server. This IP address can be used by the attacker to launch a denial-of- service (DoS) attack or to create more targeted attacks such as phishing2. With a web proxy server, the IP shown in web logs is the web proxy's, which means an attacker would not have access to theorganization's router outgoing IP address2.
Anonymizing outgoing IP addresses is also important when carrying out sensitive actions online, such as law enforcement investigations or competitive intelligence. A web proxy server can help users avoid exposing their internal IP address that leads back to their organization, and instead use a third-party web proxy that provides more anonymity2.
The other options are not directly related to reducing organizational risk by using a web proxy server. Providing multi-factor authentication for additional security (option B) is a benefit of some web proxy servers, but it is not the main purpose of using a web proxy server3. Providing faster response than direct access(option C) is a benefit of some web proxy servers that cache content forbetter data transfer speeds and less bandwidth usage, but it is not directly related to reducing organizational risk1. Load balancing traffic to optimize data pathways (option D) is a benefit of some web proxy servers that distribute traffic across multiple servers, but it is not directly related to reducing organizational risk4.
References: 1: Proxy servers and tunneling 2: Multi-factor authentication: How to enable 2FA and boost your security 3: What Is Multi-factor Authentication (MFA) Security? 4: How it works: Microsoft Entra multifactor authentication

NEW QUESTION: 259
IS □□□□ □□□□ □ □□□□ □□□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□. □□□ □□□ □□□ □ □□□ □□ □□ □□ □□□ □□□ □□ □□ □□□□ □ □□□□ □□□□.
A. □□□ □□□□ □□ □□□□ □□□□□.
B. □□□□□□□ □□□□ □□□□□.
C. □□□□ □□□ □□□□□.
D. □□ □□ □ □□□ □□□□□□□□.

Answer: (SHOW ANSWER)
The best approach for management in developing a test plan is to use processing parameters that are simulated by production entities and customers. This is because using realistic data and scenarios can help to evaluate the functionality, performance, reliability, and security of the new system under actual operating conditions and expectations. Using processing parameters that are randomly selected by a test generator, provided by the vendor of the application, or randomly selected by the user may not be sufficient or representative of the production environment and may not reveal all the potential issues or defects of the new system. References: [ISACA CISA Review Manual 27th Edition], page 266.

NEW QUESTION: 260
□□ □ □□□□ □□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□□□
C. □□□
D. □□□
Answer: B (LEAVE A REPLY)
The best method to delete sensitive information from storage media that will be reused is multiple overwriting. This is because multiple overwriting ensures that the data is practically unrecoverable by any software or hardware means. Multiple overwriting involves writing 0s, 1s, or random patterns onto all sectors of the storage media several times, making the original data unreadable or inaccessible. There arevarious software programs available that can securely delete files from storage media using multiple overwriting techniques1.
Crypto-shredding is not the best method because it only works for encrypted data. Crypto-shredding involves deleting the encryption key used to encrypt the data, making the data unreadable and unrecoverable. However, if the data is not encrypted, crypto-shredding will not erase it2.
Reformatting and re-partitioning are not the best methods because they do not erase the data completely. Reformatting and re-partitioning only delete the file system structures and pointers that make the data accessible, but thedata itself remains on the storage media and can be recovered using data recovery software

NEW QUESTION: 261
IS □□□□ □□□ □□□□ □□□□□ □□ □□□ □□□□ □□□□. □□ □ □□□ □ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□□ □□ □□ □□ □□.
B. □□ □□□ □□ □□ □□ □□ □□ □□
C. □□ □□□ □□ □□ □□ □ □□
D. □□ □□□□ □□□ □□ □ □□

Answer: A (LEAVE A REPLY)
The most important control to assess in an audit of an organization's accounts payable processes is segregation of duties between issuing purchase orders and making payments. Segregation of duties is a principle that requires different individuals or departments to perform different tasks or functions within a process, in order to prevent fraud, errors, or conflicts of interest. In the accounts payable process, segregation of duties between issuing purchase orders and making payments ensures that no one person can initiate and complete a transaction without proper authorization and verification. This reduces the risk of duplicate payments, overpayments, unauthorized payments, or payments to fictitious vendors.
References:
* Accounts payable controls
* Accounts Payable Internal Controls: A Simple Checklist

NEW QUESTION: 262
□□ □ □□□□ □□ □□ □□□□□ □□ □ □□□ □□□ □□□ □□□□□?
A. □□□□□□□□□(CISO)
B. □□□□ □□□□□
C. □□□
D. □□□□□□□(CIO)
Answer: C (LEAVE A REPLY)
Information security governance is the subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risk appropriately, uses organizational resources responsibly, and monitors the success or failure of the enterprise security program. Information security governance is essential for ensuring that an organization's information assets are protected from internal and external threats, and that the organization complies with relevant laws and standards.
Demonstrated support from which of the following roles in an organization has the most influence over information security governance? The answer is C, the board of directors. The board of directors is the highest governing body of an organization, responsible for overseeing its strategic direction, performance, and accountability. The board of directors sets the tone at the top for information security governance by:
* Establishing a clear vision, mission, and values for information security
* Approving and reviewing information security policies and standards
* Allocating sufficient resources and budget for information security
* Appointing and empowering a chief information security officer (CISO) or equivalent role
* Holding management accountable for information security performance and compliance
* Communicating and promoting information security awareness and culture The board of directors has the most influence over information security governance because it has the ultimate authority and responsibility for ensuring that information security is aligned with the organization's business objectives, risks, and stakeholder expectations.

References:
* 10: What is Information Security Governance? - RiskOptics - Reciprocity
* 11: Information Security Governance and Risk Management | Moss Adams
* 12: ISO/IEC 27014:2020 - Information security, cybersecurity and privacy ...

NEW QUESTION: 263
□□ □ □□□□□ □□□ □□□□ □□□□ □ □□□ □□ □□ □□ □□ □□□ □□ □□□?
A. □□ □□□ □□□□ □□□ □□□, □□□□□, □□□□ □□ □□□ □□□□□.
B. □□ □□□□□ □□ □□□ □□□□□ □□□ □□□□□ □□□□□.
C. □□□ ID□ □□□□ □□□□ □□□□ □□□ □□□ □□□□ □□□□□.
D. □□□ □□□ □□ □□ □□□ □□□□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
To ensurecompleteness of outbound transactions, alog with periodic validationis thebest control.
* Option A (Incorrect):Edit checkshelp withdata accuracy, not completeness.
* Option B (Incorrect):Sequential numberingdetects missing transactions but does not verifyactual transmission.
* Option C (Incorrect):Recipient ID validationis important foraccuracy, not for ensuring all transactions are sent.
* Option D (Correct):Maintaining and validating transaction logsensures thatall outbound transactions are properly accounted for, making it the best completeness control.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coversdata integrity, completeness controls, and transaction logging.

NEW QUESTION: 264
□□□ □□□□□□ □□ □□□□ □□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□ □□ □□□ □□□ □□□.
A. □□□□□□ □□□□□
B. □□□ □□□□□
C. □□□ □□□
D. □□ □□(QA) □□
Answer: (SHOW ANSWER)
In a controlled application development environment, the most important segregation of duties should be between the person who implements changes into the production environment and the application programmer. This segregation of duties ensures that no one person can create and deploy code without proper review, testing, and approval. This reduces the risk of errors, fraud, or malicious code being introduced into the production environment.

The other options are not as important as the segregation between the application programmer and the person who implements changes into production, but they are still relevant for achieving a secure and reliable application development environment. The segregation of duties between the person who implements changes into production and the systems programmer is important to prevent unauthorized or untested changes to system software or configuration. The segregation of duties between the person who implements changes into production and the computer operator is important to prevent unauthorized or uncontrolled access to production data or resources. The segregation of duties between the person who implements changes into production and the quality assurance (QA) personnel is important to ensure independent verification and validation of code quality and functionality.
References:
* ISACA CISA Review Manual 27th Edition (2019), page 247
* Segregation of Duties in an Agile Environment | AKF Partners3
* Separation of Duties: How to Conform in a DevOps World4

NEW QUESTION: 265
□□ □□ □□□ □□ □□□ □ □□□□□□□ □□□ □□□□ □□□□□□ □□□□ □ □□ □□□□ □□ □□□□□?
A. SQL □□
B. □□
C. □□
D. □□□□ □□□□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
To verify thatweb application inputs are sanitized,fuzzingis the best method because it testsvarious malformed inputsto detect security flaws.
* Option A (Incorrect):SQL injectionis a specificattack technique, not a comprehensive input validation test.
* Option B (Correct):Fuzzingis adynamic security testing techniquethat sendsrandom, malformed, or unexpected inputsto check if the application properly sanitizes and validates data.
* Option C (Incorrect):Brute forceattacks targetauthentication mechanisms, notinput sanitization.
* Option D (Incorrect):Password sprayingis an attack method, not a testing technique forinput validation.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Coverssecurity testing techniques, application security, and input validation best practices.

NEW QUESTION: 266

□□ □ □□□□ □□□ □□□□ □□□□ □□□□ □□□ □□ □□□□ □□ □□ □ □□ □□□□□?

A. □□□ □□ □□(SLA)□□ □□□□ □□ □□□ □□□□ □□□□.

B. □□□ □□ □□(SLA)□ □□□□ □□□ □□□ □□□ □□□□□.

C. □□□□□ □□□ □□□□ □□ □□ □□□□ □□□□□.

D. □□ □□ □□□ □□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

Adequate action taken for noncompliance with the service level agreement (SLA) provides the best evidence that outsourced provider services are being properly managed. This shows that the organization is monitoring the performance of the provider and enforcing the terms of the SLA.

The other options are not as convincing as evidence of proper management. Option A, the SLA includes penalties for non-performance, is a good practice but does not guarantee that the penalties are actually applied or that the performance is satisfactory. Option C, the vendor provides historical data to demonstrate its performance, is not reliable because the data may be biased or inaccurate. Option D, internal performance standards align with corporate strategy, is irrelevant to the question of outsourced provider management.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, page 2821
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription, QID 1066692

NEW QUESTION: 267

□□□ □□ □□ □□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □□□□ □?

A. □□ □□□□ □□ □□□□ □□ □□□ □□□□□.

B. □□ □□□ □□□ □□□ □□□□□ □□□□□.

C. □□ □□ □□□ □□ □□□□ □□□□.

D. □□□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 268

IS □□□□ □□ □□□ □□□ □□□ □□□□ □□ □□□ □□ □□ □□□□ □□□ □ □□□□. □□□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?

A. □□ □□□ □□□ □□□□□□□.

B. □□ □□□ □□ □□□□ □□□□□.

C. □□ □□□ □□□□□ □□□ □□□□□.

D. □□□ □□ □□□ □□□□□□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 269
BYOD(Bring Your Own Device) □□□□ □□□ □□ □□□ □□ □□ □□□□ □□ □ □□ □□□ □□□ □ □□ □□ □□ □ □□ □□□□?
A. □□ □□ □□
B. □□□ □□ □□
C. □□ □□□□□ □□□ □□ □□ □□
D. BYOD □□ □□□ □□□ □□□ □□
Answer: D (LEAVE A REPLY)
The most important input during the planning phase for an audit on the implementation of a bring your own device (BYOD) program is policies including BYOD acceptable user statements. Policies are documents that define the organization's objectives, requirements, expectations, and responsibilities regarding a specific topic or area. BYOD policies should include acceptable user statements that specify what types of personal devices are allowed to connect to the corporate network, what security measures must be implemented on those devices, what data can be accessed or stored on those devices, what actions must be taken in case of device loss or theft, and what consequences will apply for non-compliance. Policies including BYOD acceptable user statements can provide an IS auditor with a clear understanding of the scope, criteria, and objectives of the BYOD program audit. Findings from prior audits, results of a risk assessment, and an inventory of personal devices to be connected to the corporate network are also useful inputs for planning a BYOD program audit, but they are not as important as policies including BYOD acceptable user statements. References: ISACA CISA Review Manual 27th Edition, page 381.

NEW QUESTION: 270
□□□ □□□□ IT □□□□ □□□□□ □□□□ □□□□ □□ □□□ □□□□□ IT □ □□□ □□□□□. □ □□□ □□□□ □□ □□ □□ □□ □□□ □□ □ □□□□□?
A. IT □□ □□□ □□ □□□□□.
B. □□□□ □□□□□ □□□ □□□□□.
C. □□ □□ □□ □□□□ □□□□□.
D. □□□□ □□□□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The best recommendation to address the problem of missing IT deadlines on important projects because IT resources are not prioritized properly is to implement project portfolio management (PPM). PPM is the process of analyzing and optimizing the costs, resources, technologies, and processes for all the projects and programs within a portfolio. A portfolio is a collection of projects, programs, and processes that are managed together and aligned with the strategic goals and objectives of the organization. PPM can help the organization to:
Prioritize the most valuable and relevant projects and programs based on their alignment with the organizational strategy, vision, and mission.

Balance the portfolio to ensure that the projects and programs are diversified, feasible, and sustainable, and that they meet the needs and expectations of the stakeholders.
Optimize the allocation, utilization, and coordination of IT resources across the portfolio, such as staff, budget, time, equipment, and software.
Monitor and control the performance and progress of the projects and programs within the portfolio, and evaluate their outcomes and benefits.
By implementing PPM, the organization can improve its IT project delivery and avoid missing deadlines.
PPM can also help the organization to increase its efficiency, effectiveness, quality, and value. For more information about PPM, you can refer to the following web search results: Project Portfolio Management (PPM): The Ultimate Guide - ProjectManager1 A Complete Overview of Project Portfolio Management - Smartsheet2 PPM 101: What Is Project Portfolio Management?3

NEW QUESTION: 271
□□□□ □□ □□□(PMO)□□ □□□ □□ □□ □□(PIR)□ □□□□□□□ □□□ □ □ □ □□□ □ □□ □□□ □□ □ □□ □□□□?
A. □□ □□□ □□□□□□.
B. □□□□ PIR □□□□ □□□□□□.
C. □□ □□□□□□ □□□ □□□□□□.
D. □□□□ □□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
The best indicator of whether a PIR performed by the PMO was effective is whether project outcomes have been realized. Project outcomes are the benefits or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue. A PIR should evaluate whether project outcomes have been achieved in accordance with project objectives, scope, budget, and schedule. The other options are not as good as project outcomes in determining the effectiveness of a PIR. Lessons learned are valuable inputs for improving future projects, but they do not measure whether project outcomes have been realized. Management approval of the PIR report is a sign of acceptance and support for the PIR findings and recommendations, but it does not reflect whether project outcomes have been achieved. The review performed by an external provider is a way of ensuring objectivity and independence for the PIR, but it does not guarantee whether project outcomes have been realized. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 272
□□ □ □□ □□ □□ □□□□□?
A. □□□ □□□ □□ □□□□□□ □□ □□
B. □□ □□
C. □□□ □□□ □□□□ □□ □□ □□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
Verification of hash totals is a detective control. A detective control is a control that aims to identify and report errors or irregularities that have already occurred. Verification of hash totals is a technique that compares the hash values of data before and after transmission or processing to detect any changes or corruption. The other options are examples of other types of controls, such as programmed edit checks (preventive), backup procedures (recovery), and use of pass cards (preventive). References: CISA Review Manual, 27th Edition, page 223

NEW QUESTION: 273
□□ □ □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□ □□ □□
C. □□□□ □ □□ □□
D. □□ □□□□ □□□ □□
Answer: A (LEAVE A REPLY)
Issuing authentication tokens is the most reliable method of preventing unauthorized logon, as it provides a strong form of authentication that requires users to present something they have (the token) and something they know (the personal identification number or PIN) to access the system. Authentication tokens are physical devices that generate a one-time password or code that changes periodically and is synchronized with the authentication server. This makes it difficult for attackers to steal or guess the credentials of legitimate users. Reinforcing current security policies, limiting after-hours usage and installing an automatic password generator are not as reliable as issuing authentication tokens, as they do not provide a strong form of authentication and may still be vulnerable to unauthorized logon attempts. References:
* : [Authentication Token Definition]
* : Authentication | ISACA

NEW QUESTION: 274
□□ □ IS □□□□ □ □□□ □□ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □ □□□ □□□□

B. □□□□□ □□□□
C. □□ □□ □□□
D. □□□□ □□□□ □□□
Answer: D (LEAVE A REPLY)
The most significant risk that IS auditors are required to consider for each engagement is the misalignment with business objectives. This is because IS audit engagements are intended to provide assurance that the IT systems and processes support the achievement of the business objectives and strategies. If there is a misalignment,it could result in wasted resources, missed opportunities, inefficiencies, errors, or failures that could adversely affect the organization's performance and reputation12. References: 1: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.3: Audit Risk, page
28 2: CISA Online Review Course, Module 1: The Process of Auditing Information Systems, Lesson 1.3:
Audit Risk

NEW QUESTION: 275
□□ □ □□□□ □□ □□ □□(DRP)□ □□□□ □□□ □□ □ □□□□ □□ □□□□ □?
A. □□□ □□□ □□□
B. □□ □□□□ □□□
C. □□□ □□ □□
D. □□ □□ □□□
Answer: D (LEAVE A REPLY)
A disaster recovery plan (DRP) is a set of procedures and resources that enable an organization to restore its critical operations, data, and applications in the event of a disaster1. A DRP should be aligned with the organization's business continuity plan (BCP), which defines the strategies and objectives for maintaining business functions during and after a disaster1.
To ensure that a DRP is effective, it should betested regularly and thoroughly to identify and resolve any issues or gaps that might hinder itsexecution2345. Testing a DRP can help evaluate its feasibility, validity, reliability, and compatibility with the organization's environment and needs4. Testing can also help prepare the staff, stakeholders, and vendors involved in the DRP for their roles and responsibilities during a disaster3.
There are different methods and levels of testing a DRP, depending on the scope, complexity, and objectives of the test4. Some of the common testing methods are:
* Walkthrough testing: This is a step-by-step review of the DRP by the disaster recovery team and relevant stakeholders. It aims to verify the completeness and accuracy of the plan, as well as to clarify any doubts or questions among the participants45.

* Simulation testing: This is a mock exercise of the DRP in a simulated disaster scenario. It aims to assess the readiness and effectiveness of the plan, as well as to identify any challenges or weaknesses that might arise during a real disaster45.
* Checklist testing: This is a verification of the availability and functionality of the resources and equipment required for the DRP. It aims toensure that the backup systems, data, anddocumentation are accessible and up-to-date45.
* Full interruption testing: This is the most realistic and rigorous method of testing a DRP. It involves shutting down the primary site and activating the backup site for a certain period of time. It aims to measure the actual impact andperformance of the DRP under real conditions45.
* Parallel testing: This is a less disruptive method of testing a DRP. It involves running the backup site in parallel with the primary site without affecting the normal operations. It aims to compare and validate the results and outputs of both sites45.
Amongthese methods, full interruption testing would best demonstrate that an effectiveDRP is in place, as it provides the most accurate and comprehensive evaluation ofthe plan's capabilities and limitations4. Full interruption testing can reveal any hidden or unforeseen issues or risks that might affect the recovery process, such as data loss, system failure, compatibility problems, or human errors4. Full interruption testing can also verify that the backup site can support the critical operations and services ofthe organization without compromising its quality or security4.
However, full interruption testing also has some drawbacks, such as being costly, time-consuming, risky, and disruptive to the normaloperations4. Therefore, it should be planned carefullyand conducted periodically with proper coordination and communication among all parties involved4.
The other options are not as effective as full interruption testing in demonstrating that an effective DRP is in place. Frequent testing of backups is only one aspect of checklist testing, which does not cover other components or scenarios of the DRP4. Annual walk-through testing is only atheoretical review of the DRP, which does not test its practical implementation or outcomes4. Periodic risk assessment is only a preparatory step for developing or updating the DRP, which does not test its functionality or performance4.
References: 2: Best Practices For Disaster Recovery Testing | Snyk 3: Disaster Recovery Plan (DR) Testing
- Methods and Must-haves -US Signal 4: Disaster Recovery Testing: What You Need toKnow - Enterprise Storage Forum 5: Disaster Recovery Testing Best Practices - MSP360 1: How to Test a Disaster Recovery Plan - Abacus

NEW QUESTION: 276
□□□□ □□□ □, □□□□ □□□ □□□□ □□□□□ □□ □□□□ IT □□□ □□ □□□ □□□ □□□□□. IS □□□□ □ □□□ □□□ □□ □□ □□□ □□ □□□ □ □□□ □□□□ □□ □□□□□□. □□ □□□ □□□ □□□□□□□?
A. □□ □□

B. □□□ □□
C. □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
An acceptable use policy (AUP) is a preventive control that sets out rules and guidelines for using an organization's IT resources, including networks, devices, and software1. It defines acceptable and prohibited behaviors, aiming to protect assets, ensure security, and maintain a productive work environment1. By agreeing to and documenting an AUP for the equipment, both organizations can prevent potential misuse of IT resources2345.
References:
ISO 27001 Acceptable Use Policy Beginner's Guide - High Table
Acceptable Use Policy for Information Technology Resources
Acceptable Use Policies for Workplace Technology | Verizon
IT Governance: Your Must-Have Policies - How-To Geek
Acceptable use policy template - Workable

NEW QUESTION: 277
□□ □ □□□□ □□□ □□ □□□ □□ □□□□□?
A. □□ □□
B. □□□ □□
C. □□□□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
Continuous auditing is a method of performing audit-related activities on a real-time or near real-time basis.
Continuous auditing is best suited for real-time transactions, such as online banking, e-commerce, or electronic funds transfer, that require immediate verification and assurance. Low-value transactions are not necessarily suitable for continuous auditing, as they may not pose significant risks or require frequent monitoring. Irregular transactions are not suitable for continuous auditing, as they may not occur frequently or consistently enough to justify the use of continuous auditing techniques. Manual transactions are not suitable for continuous auditing, as they may not be captured or processed by automated systems that enable continuous auditing. References:
* CISA Review Manual, 27th Edition, pages 307-3081
* CISA Review Questions, Answers & Explanations Database, Question ID: 253

NEW QUESTION: 278
□□ □□ □□ □ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□ □□ □□ □□□□ □□□ □ □ □□□□?
A. □□ □□ □□ □□
B. □□□ □□□

C. □□ □□

D. □□□□ □□ □□

Answer: (SHOW ANSWER)

Using a continuous auditing module is an audit procedure that would provide the best assurance that an application program is functioning as designed. A continuous auditing module is a software tool that performs automated and continuous testing and monitoring of an application program's inputs, outputs, processes, and controls. A continuous auditing module can help to verify the accuracy, completeness, validity, reliability, and timeliness of the application program's data and transactions. A continuous auditing module can also help to identify and report any errors, anomalies, deviations, or exceptions in the application program's performance or compliance.

The other options are not as effective or relevant as using a continuous auditing module for providing assurance that an application program is functioning as designed. Interviewing business management is a technique for obtaining information and opinions from the users or owners of the application program, but it does not directly test or verify the functionality or quality of the application program. Confirming accounts is a technique for verifying the existence and accuracy of account balances or transactions, but it does not necessarily reflect the design or operation of the application program. Reviewing program documentation is a technique for examining the specifications,requirements, and procedures of the application program, but it does not provide evidence of the actual implementation or execution of the application program.

References:

* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
* Continuous audit and monitoring - PwC2

NEW QUESTION: 279

□□ □ □□□ □□□ □□□□ □□ □□□ □□□□□?

A. □□□ □□ □□□□ □□□□□.

B. □□□ □□□ □□

C. □□□ □□ □□□□ □□□□□.

D. □□□ □□□ □ □□□□ □□ □□

Answer: B (LEAVE A REPLY)

A digital signature is a mathematical algorithm that validates the authenticity and integrity of a message or document by generating a unique hash of the message or document and encrypting it using the sender's private key1. The primary reason for using a digital signature is to authenticate the sender of a message, as only the sender has access to their private key and can produce a valid signature2. A digital signature also verifies the integrity of the data, as any modification to the message or document will result in a different hash value and invalidate the signature1. However, a digital signature does not provide availability or confidentiality to the transmission, as it does not prevent denial-of-service attacks or encrypt the entire message or document3.

References
1: Understanding Digital Signatures | CISA
2: Signature Verification | CISA
3: SECFND: Digital Signatures from Skillsoft | NICCS

NEW QUESTION: 280
□□□□ □□□ □□□ □ □□ □□□ □□ □□□□□?
A. □□□□ IP□□ □□
B. □□□ □□ □□
C. □□ □□□ □□□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
The most important factor when planning a network audit is to identify the existing nodes on the network.
Nodes are devices or systems that are connected to the network and can communicate with each other. Nodes can include servers, workstations, routers, switches, firewalls, printers, scanners, cameras, etc. Identifying the existing nodes on the network will help the auditor to determine the scope, objectives, and methodology of the audit. It will also help the auditor to assess the network topology, architecture, performance, security, and compliance. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 281
□□ □ □□ □□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□□?
A. □□□ □□□ □□ □□ □□□
B. □□□ □□ □□□□ □□□ □□□ □□
C. □□□□ □□ □□ □□□ □□ □ □□
D. □□□ □□□ □□ □□ □□ □□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Forensic investigations require unaltered digital evidenceto be admissible in court.Write-protection ensures that the original data remains intact.
* Option A (Correct):Write-protecting mediapreventsaccidental or malicious changesto evidence, ensuring its integrity.
* Option B (Incorrect):Creating a digital imageis useful, but if the original evidence is modified, the integrity is lost.
* Option C (Incorrect):Hash valueshelp detect changes but donot preventthem.
* Option D (Incorrect):Chain of custodyensures accountability but doesnot physically protect the evidence.

Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets- Covers forensic principles, evidence handling, and data integrity.

NEW QUESTION: 282
□□□ □□ □□(DLP)□ □□□ □□ □□ □□□□ □□□ □□□□□ □□□ □□□□ □□ □□□□ □□□ □□□ □□□□□□. □ □□□ □□□□ □□ IS □□□□ □□□ □□ □□□ □□□□□?
A. □□□□ □□□ □□□□ □□□□□.
B. □□□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□□.
C. □□□□ □□□ □□ □□□(CASB)□ □□□□□.
D. □□□□□□ DLP □□□ □□□□ □□□ □□□ □□□□□□□.
Answer: C (LEAVE A REPLY)
Here's the breakdown, considering
the need for DLP visibility in the cloud:
Verified Answer
C: Employ a cloud access security broker (CASB).
Very Short Explanation
CASBs are specifically designed to enhance visibility and control over cloud-based data. They can monitor data flows, enforce security policies, and often have DLP capabilities built-in, making them the ideal solution in this scenario.
References
ISACA Resources (Glossary): Definitions of Cloud Access Security Broker (CASB) highlight their role in cloud security and governance.
Industry Research (Gartner, etc.): Research on CASB tools emphasizes their ability to address visibility and control challenges for cloud data.

NEW QUESTION: 283
□□ □□□□□ □□□ □□ □□ □□□ □□□ □ □□ □□□ □□□ □□□□□□□?
A. □□□
B. □□□□
C. □□
D. □□
Answer: (SHOW ANSWER)

NEW QUESTION: 284
□□ □ IT□ □□□□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□ IT □□□□ □□□ □□ □□□□□ □□□ □□
B. IT □□ □□□ □□□□ □□ □□ □□□ □□
C. IT □□ □□□ □□□□ □□□ □□
D. □□□□ □□□□ □□ □□□ □□ □□
Answer: B (LEAVE A REPLY)

The best metric to measure the alignment of IT and business strategy is the percentage of enterprise risk assessments that include IT-related risk. This metric indicates how well the organization identifies and manages the IT risks that could affect its strategic objectives and performance. A high percentage of enterprise risk assessments that include IT-related risk shows that the organization considers IT as an integral part of its business strategy and aligns its IT resources and capabilities with its business needs and goals
. References: : CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.2: IT Strategy, page 67 : CISA Online Review Course, Module 2: Governance and Management of IT, Lesson 2.2: IT Strategy

NEW QUESTION: 285
□□□ □□□□□ □□ □□ □□ □□ □□□ □□ □□ □□ □□□□□ □□□□ □□ □□ □□□ □□□ □□□□□. □□ □ □□ □□ □□□ □□ □□ □□ □□ □□□ □□ □□ □ □□ □□□□□?
A. □□ □□□
B. □□□ □□
C. □□ □□□
D. □□ □□□(VPN)
Answer: C (LEAVE A REPLY)
A load balancer is a tool or application that distributes incoming network traffic among multiple servers in a server farm, so that no server is overwhelmed and the performance of the system is optimized1. A load balancer can help the agency to handle the large influx of traffic to a regional office by balancing the workload among the available servers and preventing service disruptions. A load balancer can also provide high availability and fault tolerance by rerouting traffic to online servers if a server becomes unavailable2.
A virtual firewall is a software-based firewall that protects a virtual network or environment from unauthorized access and malicious attacks. A virtual firewall can enhance the security of the agency's network, but it does not improve the performance of its servers.
A proxy server is an intermediary server that acts as a gateway between the client and the destination server, hiding the client's IP address and providing caching and filtering functions. A proxy server can improve the security and privacy of the agency's network, but it does not improve the performance of its servers.
A virtual private network (VPN) is a secure connection between two or more devices over a public network, such as the internet. A VPN can encrypt and protect the data transmitted over the network, but it does not improve the performance of the agency's servers.

NEW QUESTION: 286
□□ □□ IT □□ □□ IT □□ □□□ □□ □□□□□, □□ □□ □□ □□□ □□□□ □ □ □□□ □□□ □□ □□ □□□ □□□ □□□□ □□ □□□ □□□□. □□ □ IS □□ □□ □□ □ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ IT □□□□ □□□□□.

B. □□□□ □□□□ □□ □□□ □□□□□.
C. □□ IT □□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□□ □□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
The best course of action for the IS auditor is A. Escalate to IT management for resolution. This is because IT management is responsible for overseeing and coordinating the IT activities and functions within the organization, and ensuring that they comply with the audit findings and recommendations1. IT management can help resolve the issue of finding ownership by:
Clarifying and communicating the roles and responsibilities of each IT team, and how they relate to the finding and its remediation2.
Evaluating and assigning the finding to the most appropriate IT team, based on their expertise, authority, and availability2.
Providing guidance and support to the assigned IT team, and monitoring their progress and performance in remediating the finding2.

NEW QUESTION: 287
□□ □□ □□□ □□ □□□□ □□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□□□□ □□□□ □□□□□.
B. □□ □□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□□□.
D. □□ □□ □□□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The primary benefit of a tabletop exercise for an incident response plan is to increase confidence in the team's response readiness (D). A tabletop exercise is a simulated scenario that tests the effectiveness and efficiency of the incident response plan and team. It allows the team to practice their roles and responsibilities, review their procedures and tools, and identify and resolve any gaps or issues in their response process. A tabletop exercise can help the team to improve their skills, knowledge, and communication, and to prepare for real incidents1.

NEW QUESTION: 288

□□□□ IT □□ □□□□ IT □□ □□□□ □□ □□□□. IT □□ □□□□ □□□□ □ □□ □ IS □□□□ □□□□ □□□ □□□ □□□ □□□□□.
A. IT□ □□□□□ □□□□ □□□ □□□□□□.
B. □□□ IT □□ □□□ □□□□□□.
C. □□□□□ □□□ □□□□ □□□□ □□□□□□.
D. IT □□□ □□□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 289
□□ □□□□□□ □□ □□□□ □□ □□□□□ □□□□□?
A. □□□□ □□
B. □□ □□□
C. □□□ □□
D. □□□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 290
□ □□□□□□□ □□□□ □□□□□ □□□□□. □□ □ □□ □□ IS □□□□□ □ □□□□□□ □□ □□□□□□ □□□□□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□
B. □ □□□□□□ □□□(WAF) □□
C. □□□□□□ □□□□□□ □□□□ □□
D. □3□□ □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 291
□□ □□ □□ IS □□□□ □□ □□□□ □□□ □□□ □□ □□ □□ □□ □□□ □□ □□□ □□ □□□□□□. □□ □ □□□□ □□□ □□ □□□ □□□□□?
A. □□ □□□□□ □□ □□□□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□□ □□□□□.
C. □□ □□□ □□□□ □□ □□ □□□□ □□□ □□ □□□□□.
D. □□□ □□□ □□□□ □□ □□□ □□ □□□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The IS auditor's best course of action is to evaluate the implemented control to ensure it mitigates the risk to an acceptable level. This is because the objective of a follow-up audit is to verify that corrective actions have been accomplished as scheduled and that theyare effective in preventing orminimizing future recurrence1. If senior management has implemented a different remediation action plan than what was previously agreed upon, the IS auditor should assess whether the alternative control is adequate and appropriate for the situation.

Requesting justification from management for not implementing the recommended control (option D) may be a secondary step, but it is not the best course of action. Reporting the deviation by the control owner in the audit report (option A) may be premature and unnecessary if the implemented control is satisfactory. Canceling the follow-up audit and rescheduling for the next audit period (option C) is not advisable, as it would delay the verification of the effectiveness of the implemented control and potentially expose the organization to further risks. References: 1: Follow-up Audits - Canadian Audit and Accountability Foundation

NEW QUESTION: 292

IS □□□□ □□ □□□ □□□ □□ □□□(IoT) □□□ □□□ □□□ □□□ □□ □□ □ □□□□ □□□□. □□ □□□ □ □□ □□ □□□ □□ □ □□ □□□ □□□□□?

A. □□ □□□ □□ Io I □□ □□□ □□□ □□□ □□□□□.

B. IoT □□ □□□ □□□□ □□□□□ □□ □□ □□

C. □□ □□□□□□ □□ IoT □□ □□□ □□ □□□ □□

D. □□ □□□□ □□□ □□□□ □□ IoT □□

Answer: B (LEAVE A REPLY)

The use of open-source software components in IoT devices presents the greatest security risk due to potential vulnerabilities that may exist within the software. These vulnerabilities can be exploited if patches are not applied promptly, and the organization might not have direct control over the software's maintenance and security updates. This risk is amplified in critical manufacturing environments where compromised IoT devices can lead to operational disruptions.

* Physical Security (Option A): While important, theft of IoT devices generally poses less risk compared to a system-wide compromise due to software vulnerabilities.
* Firmware Storage Constraints (Option C): While a limitation, this is a secondary concern compared to exploitable software.
* Devices Not Using Wireless Connectivity (Option D): Wired devices are generally more secure, reducing this as a significant concern.

Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 293

□□ □ □□□□□ □□□□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□□ □ □ □□ □□□ □□□□□?

A. □□ □□□ □□ □□ □□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□□.

B. □ □□ □□□ □□ □□ □□□□□ □□□□ □□□□□.

C. □ □□ □□□ □□□□ RAID□ □ □□□□ □□ □□□□□ □□□□ □□□ □□□ □□.

D. □ □□ □□□ □□□□ □ □□□ □□□□ □□□□□ □□□ □□□□□ □□□□ □.

Answer: B (LEAVE A REPLY)
Configuring each authentication server as belonging to a cluster of authentication servers is the best way to minimize performance degradation of servers used to authenticate users of an e-commerce website. A cluster is a group of servers that work together to provide high availability, load balancing, and fault tolerance. If one server fails or becomes overloaded, another server in the cluster can take over its workload without disrupting the service. A single server as a primary authentication server and a second server as a secondary authentication server is not as effective as a cluster, because the secondary server is only used when the primary server fails, which means it is idle most of the time and does not improve performance. Configuring each authentication server and ensuring that each disk of its RAID is attached to the primary controller does not address the issue of performance degradation, but rather the issue of data redundancy and reliability. RAID (redundant array of independent disks) is a technology that combines multiple disks into a logical unit that can tolerate disk failures and improve data access speed. Configuring each authentication server and ensuring that the disks of each server form part of a duplex does not address the issue of performance degradation, but rather the issue of data backup and recovery. A duplex is a pair of disks that store identical copies of data, so that if one disk fails, the other disk can be used to restore the data. References: ISACA CISA Review Manual 27th Edition, page 310

NEW QUESTION: 294
□□ □□ □□□□ □□ IS □□□□ □□ □□□ □□□□□□ □□□ □□□ □□□□ □□□□□. □□□□ □□□ □□ □□□ □□□□□?
A. IT □□□□ □□□□.
B. □□□□ □□ □□□ □□□□□.
C. □□ □□□□ □□ □□□ □□□□□.
D. □□ □□□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 295
□□ □□ □□ IS □□□□ □ □□ □□□ □□ □□□ IS □□□□ □□□ □□ □□□□ □□□□□?
A. □□ □□□□□ □□ □□□ □□ □□□□ □□□□□.
B. □□ □□ □□□ □□ □□ □□□□□.
C. □□ □□□□ □□ □□ □□□ □□□□□.
D. □□□□ □□ □□□ □□ □□ □□□□□ □□□□□□□.
Answer: C (LEAVE A REPLY)
The best course of action for an IS auditor who finds that some critical recommendations have not been implemented is to evaluate senior management's acceptance of the risk. The IS auditor should understand the reasons why the recommendations have not been implemented and the implications for the organization's risk exposure. The IS auditor

should also verify that senior management has formally acknowledged and accepted the residual risk and has documented the rationale and justification for their decision. The IS auditor should communicate the findings and the risk acceptance to the audit committee and other relevant stakeholders. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 296
□□ □ IT □□□□□ □□□ □□□ □□ □□ □□ □□□ □□□□ □□ □□□□□?
A. □□□□ □□□ □□□ □□ IT □□□□□□ □□□□□□□.
B. IT □□□□□□ □□ □□ □□□□□ □□□□ □□□□□□□.
C. IT □□□□□□ □□□□□ □ □□ □□□□ □□□□□ □□□□□.
D. IT □□□□□ □□□□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 297
□□ □ □□□ □□□□□□ □□□□□ □ □□ □□□ □□□□□?
A. □□□ □□□□□ □□□□ □□□□□ □□□ □□□ □□□□ □□ □□ □□
B. □□□□ □□□□ □□ □□ □□□□□□□ □□□ □□□ □□□□□.
C. □□□ □□□□ □□□ □□ □□
D. □□□ □□ □□□□ □□
Answer: C (LEAVE A REPLY)
Data migration is the process of moving data from one system to another, which may involve changes in storage, database, or application. To perform a successful data migration, it is essential to understand the data structure of the new system, which defines how the data is organized, stored, and accessed. Understanding the new system's data structure will help determine the following aspects of the data migration project:
The scope and requirements of the data migration, such as what data needs to be migrated, how much data needs to be migrated, and what are the quality and performance expectations.
The data mapping and transformation rules, such as how the data elements from the source system correspond to the data elements in the target system, and what transformations or conversions are needed to ensure compatibility and consistency.
The data validation and testing methods, such as how to verify that the migrated data is accurate, complete, and functional in the new system, and how to identify and resolve any errors or issues.
Therefore, understanding the new system's data structure is a crucial first step in a data migration project, as it lays the foundation for the subsequent steps of data extraction, transformation, loading, validation, and testing.

NEW QUESTION: 298

□□□ □□ □□□□□ □□□ □□□ □□□ □ IS □□□□ □□□ □□□□ □□□.
A. □□□□ □□ □□ □□□ □□□ □□□□□.
B. □□ □□(RFP)□ □□□□ □□ □□□ □□□□□ □□□□□.
C. □□-□□ □□□ □□□□ □□□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□□□□ □□□.
Answer: (SHOW ANSWER)
A feasibility study is an assessment that determines the likelihood of a proposed project being successful, such as a new system development1. A feasibility study typically covers various aspects of the project, such as technical, economic, operational and legal feasibility2. The IS auditor's role is to audit the feasibility study and ensure that it is objective, realistic and reliable3.
One of the most important aspects of a feasibility study is the economic feasibility, which analyzes the costs and benefits of the proposed system and compares them with alternative solutions2. Theeconomic feasibility study should include a detailed breakdown of the development, implementation and operational costs, as well as the expected revenues, savings and intangible benefits of the system3. The IS auditor should review the cost-benefit documentation for reasonableness and accuracy, and verify that the assumptions and calculations are valid and supported by evidence3.
The other options are not directly related to auditing the feasibility study of a system development project.
Reviewing qualifications of key members of the project team (option A) is more relevant to auditing the project management and human resources aspects of the project. Reviewing the request for proposal (RFP) to ensure that it covers the scope of work (option B) is more relevant to auditing the procurement and vendor selection process of the project. Ensuring that vendor contracts are reviewed by legal counsel (option D) is more relevant to auditing the legal and contractual aspects of the project.
References: 3: Types of Feasibility Study in Software Project Development 2: Feasibility Analysis in System Development Process 1: What Is a Feasibility Study? Definition, Benefits and Types

NEW QUESTION: 299
□□ □ □□□ □□□□□ □□ □□□□□ □□ □□ □□□ □□ □□ □□ □□□ □□ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□ □□ □□□ □ □□ □□ □□ □□
B. □□ □□□□ □□□ □ □□ □□□□ □ □□□ □□
C. □□□ □□□□ □□□□□ □□ □□ □□(SDLC) □□□□ □□
D. □□□□□ □□□□ □□ □□□□□ □□□ □□□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 300
IT □□□□□ □□□□ □□ □□□ □□ □□□ □□□ □□□□.

A. □□ □□ □□
B. □□□□ □□□□.
C. □□□ □□□□□□.
D. □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The primary objective of value delivery in reference to IT governance is to optimize investments. Value delivery is one of the five focus areas of IT governance that aims to ensure that IT delivers expected benefits to stakeholders and enables business value creation. Value delivery involves aligning IT investments with business objectives and strategies, managing IT performance and benefits realization, optimizing IT costs and risks, and enhancing IT innovation and agility. Value delivery helps to maximize the return on investment (ROI) and value for money (VFM) of IT resources and capabilities.
References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 301
□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□□ □□□.
A. □□ □□ □□□□.
B. □□ □□ □□.
C. □□□□□□ □□□□(EA).
D. □□ □□□□ □□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 302
□ □□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□□□ □□□□ □ □□□□□. □□ □ □□ □□ IS □□□□ □□□□ □□ □□ □□□ □□□ □□ □ □□ □□□□?
A. □□ □□□□ □□□□ □□ □□□ □ □□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□□□ □□ □□ □ □□ □□ □□□□ □□□□□.
C. □□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.
D. □□□□ □□□□ □□ □□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)
Reviewing input and output control reports to verify the accuracy of the system decisions is the most important procedure for the IS auditor to perform during the post-implementation review of intelligent-agent software for granting loans to customers, because it can help identify any errors or anomalies in the system logic or data that may affect the quality and reliability of the system outcomes. Reviewing system and error logs, signed approvals, and system documentation are also important procedures, but they are not as critical as verifying the accuracy of the system decisions. References: CISA Review Manual (Digital Version), Chapter
4, Section 4.2.21

NEW QUESTION: 303
□□ □ □□□ IS □□□□□ □□□□ IT □□□ □□□□ □ □□ □□□ □□□ □□□ □ □□ □□□□□?
A. IT □□ □□
B. □□ □□ □□□
C. IT □□ □□□
D. □□□ □□ □□□
Answer: C (LEAVE A REPLY)
An IT balanced scorecard (BSC) is a performance metric that is used to identify, improve, and control the various functions and outcomes of an IT department or organization. An IT BSC is based on the concept of the balanced scorecard, which was introduced by Robert Kaplan and David Norton in 1992 as a strategic management system that translates the vision and strategy of an organization into measurable objectives and actions. An IT BSC adapts the balanced scorecard framework to the specific needs and goals of the IT function, aligning it with the business strategy and value proposition.
An IT BSC typically consists of four perspectives that help managers plan, implement, and evaluate the IT performance: customer, internal process, learning and growth, and financial. Each perspective defines a set of objectives, measures, targets, and initiatives that reflect the IT contribution to the organization's success. For example, the customer perspective may measure the satisfaction and retention of internal and external customers who use IT services or products; the internal process perspective may measure the efficiency and effectiveness of IT processes such as development, delivery, support, or security; the learning and growth perspective may measure the skills, knowledge, innovation, and culture of the IT staff; and the financial perspective may measure the costs, benefits, and return on investment of IT projects or assets.
An IT BSC provides a new IS auditor with the most useful information to evaluate overall IT performance because it:
* Provides a comprehensive and balanced view of the IT function from multiple angles and stakeholders
* Links the IT objectives and activities to the business strategy and value creation

* Enables a clear communication and alignment of expectations and priorities among IT managers, staff, customers, and other stakeholders
* Facilitates a continuous monitoring and improvement of IT performance based on data-driven feedback and analysis
* Supports a holistic and integrated approach to IT governance, risk management, and compliance Therefore, an IT BSC is a valuable tool for a new IS auditor to assess how well the IT function is fulfilling its mission and delivering value to the organization.
References:
* The IT Balanced Scorecard (BSC) Explained - BMC Software
* What Is a Balanced Scorecard (BSC), How Is it Used in Business?
* Lost in the Woods: COBIT 2019 and the IT Balanced Scorecard - ISACA

NEW QUESTION: 304
□□□ □□□ □□ □□ □□□ □□□ □□ □□□□ □□□□□ □□□ □□□□□. □ □ □ □□ □□ □ □□□□□ □□ □□□ □□□ □□□?
A. □□□ □□□
B. □□□ □□ □□
C. □□ □□□
D. □□ □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 305
□□□ □□ □□ □□□□□ □□□□ IS □□□□ □□ □□□□ □□□□ □ □□□ □ □□□□?
A. □□ □ □□ □□□ □□□□ □□ □□□ □□□□□□□.
B. □□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□□ □□□□.
C. □□□ □□ □□ □□□□ □□□□□.
D. □□□ □□□□ □□ □□□ □□□□ □□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 306
□□ □ □□ □□□ □□□□□ □□□□ □□□ □ □□ □□□□ □□ □□□ □□□□ □?
A. □□ □□□□□ □□□
B. □□ □□ □ □□ □□□□
C. □□□ □□□ □ □□ □
D. □ □□ □□ □
Answer: A (LEAVE A REPLY)
The executive management concern that could be addressed by the implementation of a security metrics dashboard is the effectiveness of the security program. A security metrics dashboard is a tool that provides a visual representation of key performance indicators

(KPIs) and key risk indicators (KRIs) related to the organization's information security objectives and activities. A security metrics dashboard can help executive management monitor and evaluate the performance and value delivery of the security program, identify strengths and weaknesses, assess compliance with policies and standards, and support decision making and improvement initiatives. Security incidents vs. industry benchmarks, total number of hours budgeted to security, and total number of false positives are not executive management concerns that could be addressed by the implementation of a security metrics dashboard. These are more operational or technical aspects of information security that could be measured and reported by other means, such as incident reports, budget reports, or log analysis. References: [ISACA CISA Review Manual 27th Edition], page 302

NEW QUESTION: 307
IS □□□□ □□ □□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□. □□ □ □□ □□ □ □□□□ □□□ □□□□□□ □□□□ □ □□ □□ □□□ □□□□□?
A. □□□ □□□ □□□ □□
B. □□□ □□□□□ □□□
C. □□□ □□ □□□□ □□
D. □□□ □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 308
□□ □ □□ □ □□ □□□ □□ □□□□□ □□□□ □□ □□□□□?
A. □□□□
B. □□□ □□
C. □□□ □□
D. □□ □□□
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:Transposition and transcription errors occur when characters or numbers are accidentally swapped or misentered during data entry.
* Option A (Incorrect):Duplicate checks ensure that the same record is not entered twice but do not specifically detect transposition or transcription errors.
* Option B (Incorrect):Completeness checks ensure that all required data is entered but do not validate data accuracy.
* Option C (Incorrect):Sequence checks verify that records follow a logical sequence but do not catch errors within individual data entries.
* Option D (Correct):Acheck digitis an additional number generated through an algorithm (e.g., Luhn algorithm for credit cards) that helps detect errors such as transpositions (e.g., swapping digits 45 # 54) and transcriptions (e.g., mistyping 8 as 3).

Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Covers input validation and error detection techniques.

NEW QUESTION: 309
□□ □□□ □□□□ □□□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□?
A. □□
B. □□□
C. □□
D. □□
Answer: A (LEAVE A REPLY)
A biometric access device installed at the entrance to a facility is a type of preventive control. Preventive controls are designed to deter or prevent undesirable events from occurring12. They are proactive measures that aim to inhibit incidents before they happen12. In this case, the biometric access device prevents unauthorized individuals from gaining access to the facility by requiring unique biological characteristics for authentication12.
References:
Guide to Biometric Access Control & Door Lock Security - Avigilon
Biometric access control: meaning, types and implementation - Smowl

NEW QUESTION: 310
□□ □ □□□ □□□ □□□ □□□ □□□□□□ □□□□ □□□ □□□□ □□ IS □ □□□ □□ □□ □□ □□□□□ □□□□□?
A. □□□□□□□(IPS) □ □□□
B. □□□ □□ □□(DLP) □□
C. □□□ □□
D. □□□ □□ □□□□□ □□
Answer: B (LEAVE A REPLY)
DLP technologies are designed to prevent the unauthorized transmission or leakage of sensitive data, such as PII, intellectual property, or financial information, by employees or other insiders. DLP technologies can monitor, detect, and block data in motion, data at rest, and data in use across various channels, such as email, web, cloud, or removable devices. DLP technologies can also help enforce data security policies and compliance requirements.
References
ISACA CISA Review Manual, 27th Edition, page 253
The role of disclosures in risk assessment and mitigation
Mitigate Risk Strategy for Information Management

NEW QUESTION: 311

□□ □□□ □□ □□□ □□□ □□□ □□□□□□ □□□□ □□, □□□□ IT □□□□ □□□□□□ □□□□ □□ □□ □ □□□ □□□□□?
A. □□□, □□ □ □□ □□□□ □□ □□ □□ □□□ □□□
B. IT □□□□□ □□ □□□□□ □□□ □□ □ □□ □□□ □□ □□□□ □□
C. □□ □□□□ □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□
D. IT □□□□ □□□ □□ □□□ □□□□ □ □□ □□□□ □□□ □□
Answer: D (LEAVE A REPLY)
The greatest benefit of adopting an international IT governance framework rather than establishing a new framework based on the actual situation of a specific organization is wide acceptance by different business and support units with IT governance objectives. An international IT governance framework, such as COBIT, provides a common language and understanding for IT governance among various stakeholders, such as management, users, auditors and regulators. This facilitates alignment, communication and collaboration among them. Readily available resources, comprehensive coverage and fewer resources expended are also benefits of adopting an international IT governance framework, but they are not the greatest benefit. References: CISA Review Manual (Digital Version) , Chapter 1, Section 1.3.1.

NEW QUESTION: 312
□□ □ IS □□□□ □□□ □□ □□□ □□ □□□□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□
B. □□ □□
C. □□□□□□ □□
D. □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 313
□□ □□ □□□□□ □□□ □□□□ □□ IS □□□□ □□□ □□□ □□□ □□□□□ □□□ □□□□ □□□ □□□ □□ □□□□□□ □□ □□□□□. □□ □ □□□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□ □□□ □□ □□□□ □□□□□.
B. □□ □□□ □□□ □□□ □□□ □□□□□.
C. □□ □□□ □□□□□ □□□□ □□□□ □□ □□□□□ □□□□□.
D. □□ □□ □□□ □□ □□□□ □□ □□□□□ □□ □□ □□□ □□□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 314
□□□□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□□□□. □□ □ □□ □ □ □□□ □ □□□ □□ □ □□□ □□□□□?

A. □□□□□□ □□□□ □□□□ □□□□□ □□□□□.
B. □□□ □□□□□ □□□□□ □□□□□.
C. □□ □□□ □□□ □□□ □□ □□□□□.
D. □□□□□□ □□□□ □□□□□ □□□ □ □□□□.
Answer: D (LEAVE A REPLY)
The programmer having access to the production programs is the most likely control weakness that would have contributed to the unauthorized changes to the payroll system report. This is because the programmer could modify the production code without proper authorization, documentation, or testing, and bypass the change management process. This could result in errors, fraud, or data integrity issues in the payroll system.
The programmer should only have access to the development or test environment, and the production programs should be under the control of a librarian or a change manager.
References
ISACA CISA Review Manual, 27th Edition, page 254
4 Types of Internal Control Weaknesses
ACCT 4631 - Internal Auditing: CIA Quiz Topic 6 Flashcards

NEW QUESTION: 315
□□ □□ □□ □□□□□ □□□□ IS □□□□ □□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□□□□□. □□ □ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□□□ IT □□□ □ □□□□□□ □□ □□□ □□□□□.
B. □□ □□ □ □□□ □□(SIEM) □□□□ □□ □□□ □□
C. □□ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The auditor's best recommendation is D. Introduce problem management into incident response. Problem management is a practice that aims to identify, analyze, and resolve the root causes of recurring incidents, and prevent or reduce their impact in the future1. Problem management can help improve the resolution times for recurring incidents by eliminating or mitigating the underlying problems that cause them, and by providing permanent solutions that can be reused or automated2. Problem management can also help improve the quality and efficiency of incident response by reducing the workload and complexity of dealing with repetitive issues2.

NEW QUESTION: 316
□□ □ IT □□ □□□□ □□ □□□ □□□□□?
A. □□□□ □□ □□□ □□ IT □□□□□ □□ □□ □□
B. □□□ IT □□ □□ □□
C. IT □□ □□□ □□ □□ □□ □ □□□□
D. □□□□□ □□ IT □□ □□
Answer: A (LEAVE A REPLY)

A primary responsibility of an IT steering committee is prioritizing IT projects in accordance with business requirements, as this ensures that IT resources are allocated to support the strategic objectives and needs of the organization. Reviewing periodic IT risk assessments, validating and monitoring the skill sets of IT department staff, and establishing IT budgets for the business are important activities, but they are not the primary responsibility of an IT steering committee. They may be delegated to other IT governance bodies or functions within the organization. References: CISA Review Manual (Digital Version), Chapter 1:
Information Systems Auditing Process, Section 1.2: IT Governance

NEW QUESTION: 317
IS □□□□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□□ □□□□ □□□□□ □□ □□□ □□□□ □ □□□ □□□.
B. □□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□□□ □ □□ □□ □□ □□□ □□ □□□ □□□□.
D. □□ □□ □□□□ □□□ □□ □□□ □□□ □□□□ □ □□□ □□□.
Answer: A (LEAVE A REPLY)
The primary reason for an IS auditor to perform a risk assessment is to help identify areas with a relatively high probability of material problems. A risk assessment is a systematic process of evaluating the potential risks that may be involved in an activity or undertaking. It involves identifying the sources of risk, analyzing the likelihood and impact of the risk, and prioritizing the risks based on their significance. A risk assessment helps the IS auditor to focus on the areas that are most vulnerable to errors, fraud, or inefficiencies, and to design appropriate audit procedures to address those risks. A risk assessment also helps the IS auditor to allocate audit resources efficiently and effectively.
A risk assessment does not provide a basis for the formulation of corrective action plans, as this is a responsibility of management, not the IS auditor. A risk assessment does not increase awareness of the types of management actions that may be inappropriate, as this is a matter of professional ethics and judgment. A risk assessment does not help to identify areas that are most sensitive to fraudulent or inaccurate practices, as this is a result of the risk assessment, not its purpose.
References:

ISACA, CISA Review Manual, 27th Edition, Chapter 1: The Process of Auditing Information Systems, Section 1.3: Risk Assessment in Planning1 Corporate Finance Institute, Audit Risk Model2

NEW QUESTION: 318
□□ □ IS □□□□ □□□ IT □□□ □□□ □□□ □□□ □□□ □□□□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□□□□ □□□□(EA)
B. □□ □□ □□(BIA)
C. □□□ □□ □□□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
Enterprise architecture (EA) is the most helpful to an IS auditor reviewing the alignment of planned IT budget with the organization's goals and strategic objectives. EA is a well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a comprehensive approach at all times, for the successful development and execution of strategy1. EA provides a blueprint for an effective IT strategy and guides the controlled evolution of IT in a way that delivers business benefit in a cost-effective way2. By reviewing the EA, the IS auditor can evaluate how well the planned IT budget supports the business vision, strategy, objectives, and capabilities of the organization.
The other options are not as helpful as EA for reviewing the alignment of planned IT budget with the organization's goals and strategic objectives. BIA is a process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption3. BIA quantifies the impacts of disruptions on service delivery, risks to service delivery, and recovery time objectives (RTOs) and recovery point objectives (RPOs)3. BIA is useful for developing strategies, solutions, and plans for business continuity and disaster recovery, but it does not directly address the alignment of planned IT budget with the organization's goals and strategic objectives. Risk assessment report is a document that contains the results of performing a risk assessment or the formal output from the process of assessing risk4. Risk assessment is a method to identify, analyze, and control hazards and risks present in a situation or a place5. Risk assessment report is useful for identifying and mitigating potential threats and issues that are detrimental to the business or an enterprise, but it does not directly addressthe alignment of planned IT budget with the organization's goals and strategic objectives. Audit recommendations are guidance that highlights actions to be taken by management6. When implemented, process risks should be mitigated, and performance should be enhanced6. Audit recommendations are useful for improving the quality and reliability of the information system and its outputs, but they do not directly address the alignment of planned IT budget with the organization's goals and strategic objectives. Therefore, option A is the correct answer.

NEW QUESTION: 319
□□ □ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□ □□(DLP) □□□□□ □□
B. □□ □□□ □□ □□
C. □□□□ □□ □□ □□ □□ □□
D. □□ □□ □□□□ □□
Answer: D (LEAVE A REPLY)
The most effective way to identify exfiltration of sensitive data by a malicious insider is to establish behavioral analytics monitoring. Behavioral analytics is the process of analyzing the patterns and anomalies in user behavior to detect and prevent insider threats. Behavioral analytics can help identify unusual or suspicious activities, such as accessing sensitive data at odd hours, transferring large amounts of data to external devices or locations, or using unauthorized applications or protocols. Behavioral analytics can also help correlate data from multiple sources, such as network logs, user profiles, and access rights, to provide a holistic view of user activity and risk.
Data loss prevention (DLP) software is a tool that can help prevent exfiltration of sensitive data by a malicious insider, but it is not the most effective way to identify it. DLP software can block or alert on unauthorized data transfers based on predefined rules and policies, but it may not be able to detect sophisticated or stealthy exfiltration techniques, such as encryption, steganography, or data obfuscation.
Reviewing perimeter firewall logs is a way to identify exfiltration of sensitive data by a malicious insider, but it is not the most effective way. Perimeter firewall logs can show the traffic volume and destination of data transfers, but they may not be able to show the content or context of the data. Perimeter firewall logs may also be overwhelmed by the amount of normal traffic and miss the signals of malicious exfiltration.
Providing ongoing information security awareness training is a way to reduce the risk of exfiltration of sensitive data by a malicious insider, but it is not a way to identify it. Information security awareness training can help educate users on the importance of protecting sensitive data and the consequences of violating policies and regulations, but it may not deter or detect those who are intentionally or maliciously exfiltrating data.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 300
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription 1
* Cybersecurity Engineering for Legacy Systems: 6 Recommendations - SEI Blog 2
* How to Secure Your Company's Legacy Applications - iCorps

NEW QUESTION: 320
IS □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□. □□ □ □□ □□□ □□ □□□ □□□□□?

A. □□□□□□ □□ □□
B. □□ □□ □□□ □□□ □□
C. □□ □□□ □□□
D. □□□□ □□ □□
Answer: C (LEAVE A REPLY)
The most important consideration when assessing the adequacy of management's remediation action plan is the criticality of the audit findings, as this reflects the level of risk and impact that the findings pose to the organization's objectives, performance, and value. The IS auditor should evaluate whether the remediation action plan addresses the root causes, mitigates the risks, and resolves the issues of the audit findings in a timely and effective manner. The IS auditor should also consider the feasibility, reasonableness, and measurability of the remediation actions.
References
ISACA CISA Review Manual, 27th Edition, page 256
How to Write an Audit Finding - Dallas Chapter of the IIA
How to Write an Audit Report: 14 Steps (with Pictures) - wikiHow

NEW QUESTION: 321
□□ □□□ □□ □□ □□ □ □□ □□ □□□□ □□□ □□ □□ □□□ □□□□ □ □ □ □□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□(CSA)
D. □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 322
□□□ □□ □□□ □□□ □□□ IT □□□□ □□□ □□□ □□□□□. □□□ □□□ □□□ □□□□ □□□□□□□ □□□□□□□. □□ □ IS □□□□□ □□ □□□□ □ □□ □□□□□?
A. □□□ □□□ □□
B. □□ □□□ □□
C. □□□□ □□ □□ □□□□□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 323
□□ IT □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□ □ □□ □□
B. □□□ □□ □□□(UAT) □□
C. □□□ □□ □□

D. □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 324
□□ □□□□□ □□ □□□ □□□ □, □□ □ □□ □□ □□ □ □□ □□□□□?
A. □□□ □□ □□□□ □□□ □□□□□.
B. □ □□ □□□ □□□□□.
C. □□ □□□□□ □□□□.
D. □□□ ID □□□□□.
Answer: D (LEAVE A REPLY)
The first thing that should be done when an intrusion into an organization network is detected is to identify nodes that have been compromised. Identifying nodes that have been compromised is a critical step in responding to an intrusion, as it helps determine the scope, impact, and source of the attack, and enables the implementation of appropriate containment and recovery measures. The other options are not the first things that should be done when an intrusion into an organization network is detected, as they may be premature or ineffective without identifying nodes that have been compromised. Blocking all compromised network nodes is a containment measure that can help isolate and prevent the spread of the attack, but it may not be possible or feasible without identifying nodes that have been compromised. Contacting law enforcement is a reporting measure that can help seek external assistance and comply with legal obligations, but it may not be necessary or appropriate without identifying nodes that have been compromised. Notifying senior management is a communication measure that can help inform and escalate the incident, but it may not be urgent or accurate without identifying nodes that have been compromised. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2

NEW QUESTION: 325
□□□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□
B. □□□□ □□□□□ □□ □□ □□□□ □□□□.
C. □□ □ □□□□ □□□□ □□ □□□ □□□ □□□□.
D. □□ □□ □□ □ □□ □□□□□ □□□□.
Answer: (SHOW ANSWER)
The most critical finding when reviewing an organization's information security management is no periodic assessments to identify threats and vulnerabilities. Periodic assessments are essential for ensuring that the organization's information security policies, procedures, standards, and controls are aligned with the current and emerging risks and threats that may affect its information assets. Without periodic assessments, the organization may not be aware of its actual security posture, gaps, or weaknesses, and may not be able to take appropriate measures to mitigate or prevent potential security

incidents. No dedicated security officer, no official charter for the information security management system, and no employee awareness training and education program are also findings that may indicate some deficiencies in the organization's information security management, but they are not as critical as no periodic assessments to identify threats and vulnerabilities. References: ISACA CISA Review Manual 27th Edition, page 343.

NEW QUESTION: 326
IS □□□□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□ □□□□ 5□ □□ □□ □ □□ □□□ □□ □□□□□. □□□□ □□ □ □□□ □□□□ □□ □□□?
A. □□□□□□ □□ □□□□□ □□□□□.
B. □□ □□□□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□□ 100%□ □□□□.
D. □□ □□□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
An IS auditor is analyzing a sample of accounts payable transactions for a specific vendor and identifies one transaction with a value five times as high as the average transaction. The next step that the auditor should do is to request an explanation of the variance from the auditee. This is because the variance may indicate an error, fraud, or an unusual but legitimate transaction that requires further investigation. The auditor should not report the variance immediately to the audit committee without verifying its cause and significance. The auditor should not increase the sample size to 100% of the population without considering the cost-benefit analysis and the sampling methodology. The auditor should not exclude the transaction from the sample population without justification, as itmay affect the validity and reliability of the audit results. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 327
□□ □□ □□ IS □□□□ □□□□□□ □□ □□ □□□(IPS)□□ □□ □□ □□□ □ □□□ □□□ □□□□. □□□□ IPS □□□ □□□ □□□ □ □□ □□□ □□□ □□□ □ □□ □□□□ □□□ □□ □□□ □□□□□?
A. □□□ □□
B. □□ □□
C. □□ □□
D. □□□ □□
Answer: B (LEAVE A REPLY)
The type of risk associated with the potential for the auditor to miss a sequence of logged events that could indicate an error in the IPS configuration is detection risk. Detection risk is the risk that the auditor's procedures will not detect a material misstatement or error that exists in an assertion or a control. Detection risk can be affected by factors such as the nature, timing, and extent of the audit procedures, the quality and sufficiency of the audit evidence, and the auditor's professional judgment and competence. Detection risk can be

reduced by applying appropriate audit techniques, such as sampling, testing, observation, inquiry, and analysis. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 328
□□□□ □□ □ □□□(PKI)□ □□□□ □□□ □□□ □□□□□. □□□ □□□□ □ □ □□ □□□□□□ □□□□ □□ □□□□ □□□ □□ □ □□ □□□□?
A. □□□□ □□ □□□□□ □□□□ □□□□□□.
B. □□□□ TLS(□□ □□ □□) □□□□□ □□□□ □□□□□.
C. □□□□ □□□□ □□□□ □□□ □□ □□□□□.
D. □□□□ □□□□ □□ □□ □□□□ □□□□□□.
Answer: (SHOW ANSWER)
This method is known as creating a digital signature of the message. It ensures the integrity of the message by verifying that it has not been tampered with in transit. The process involves hashing the message and encrypting the hash value with the sender's private key. Any changes to the message will result in a different hash value1. This method is used in DomainKeys Identified Mail (DKIM), which verifies an email's domain and helps show that the email has not been tampered with in transit2.
References:
Understanding Digital Signatures | CISA
Using DomainKeys Identified Mail (DKIM) in your organisation

NEW QUESTION: 329
□□□ □□ □□ □□□(QMS)□ □□ □□□ □□□ □ IS □□□□ □□□□ □ □□ □ □□ □□ □□□□□?
A. □□□ □□□□ □□□□ □□□ □□ □□□□□□ □□□□ □□
B. □□ □□□□ □□□□□□ □□ □□□ □□□□ □□□□□ □□
C. □□□□ □□ □□ □ □□□ □□□ □□□□□□ □□□□□ □□□ □□
D. □□□ □□ □□ □ □□□ □□□ □□ □□ □□ □□□ □□□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 330
□□ □ IS □□ □□□□ □□□□ □□□□ □□ □□ IS □□□ □□□ □□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□□□□ □□
B. □□ □□ □□ □□□ □□□ □□□ □□□□□□ □□□□ □□
C. □□□ □□□ □□□□□ □□□□□□ □□□□ □□
D. □□□ □□ □□□ □□ □□□□□ □□□□ □□
Answer: A (LEAVE A REPLY)

The primary reason for an IS audit manager to review the work performed by a senior IS auditor prior to presentation of a report is to ensure the conclusions are adequately supported. The IS audit manager is responsible for overseeing and supervising the audit process, ensuring the quality and consistency of the audit work, and approving the audit report and recommendations. The IS audit manager should review the work performed by the senior IS auditor to verify that the audit objectives, scope, and criteria have been met, that the audit evidence is sufficient, reliable, and relevant, and that the audit conclusions are logical, objective, and based on the audit evidence. The IS audit manager should also ensure that the audit report is clear, concise, accurate, and complete, and that it communicates the audit findings, conclusions, and recommendations effectively to the intended audience. The other options are not the primary reason for an IS audit manager to reviewthe work performed by a seniorIS auditor prior to presentation of a report, because they either relate to specific aspects or stages of the audit work rather than the overall outcome, or they are part of the senior IS auditor's responsibility rather thanthe IS audit manager's. References: CISA Review Manual (Digital Version)
1, Chapter 2, Section 2.2.5

NEW QUESTION: 331
IS □□□□ □□□ □□ □□□ □□□ □ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□ □□□□ □ □□ □□□ □□□ □□ □□□ □□□□ □□□ □□□□.
B. □□□□ □□ □□ □□□ □□ □□□ □□□□.
C. □□□□ □□ □□ □□(NDA)□ □□□□□ □□□□ □□□ □□□□.
D. □□□ □□□ □□□ □ □□ □□□ □□□ □□□□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Failure torevoke access upon terminationposes the greatest security risk, as ex-employees could still access sensitive data or systems.
* No Policy to Revoke Access (Correct Answer - A)
* A terminated employee retaining access can lead todata breaches or insider threats.
* Example:A former employee misuses active credentials to access financial systems.
* Lack of Security Awareness Training (Incorrect - B)
* Important but does not pose an immediate security risk like an active ex-employee account.
* No NDAs (Incorrect - C)
* Protects intellectual property but is not as critical as system access.
* No Access Revocation for Role Changes (Incorrect - D)
* Still a concern, but ex-employees with active access are ahigherrisk.
References:
* ISACA CISA Review Manual
* NIST 800-53 (Access Control)

NEW QUESTION: 332
□□□□ □3□□ □□□□ □□□□□ □□□ □□□ □□□□ □□□□□□□ □□□□ □□. □□ □ □□□□□□□ □□□ □□□ □□□□□ □□□□ □ □□ □□□ □□□ □□ □□□□□?
A. □□□□□□(KPI) □□□□
B. □□ □□
C. □□ □□
D. □□ □□(QA)
Answer: (SHOW ANSWER)
The most important process to help ensure the application provides accurate calculations is quality assurance (QA), which involves verifying that the application meets the specified requirements and standards, and testing the application for functionality, performance, reliability, security, and usability. QA helps to identify and correct any defects or errors in the application before it is deployed to the production environment. Key performance indicator (KPI) monitoring, change management, and configuration management are important processes for managing and maintaining the application after it is implemented, but they do not directly ensure the accuracy of the calculations performed by the application. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.3:
Practices for Quality Assurance

NEW QUESTION: 333
□□ □□ □□□□ □□□ IT □□ □□□ □□ □□□ □□□□□□. □□ □□□ □□□ □ □□ □□□ □□ □□□ □□ □ □□ □□□□?
A. □□ □□ □□□ □□□ □□□ □□□ □□□□□.
B. □□□ □□□ □□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□□ □□
D. □□ □□ □□□ □□□ □□ □□□□□.
Answer: (SHOW ANSWER)
The most important consideration when planning the next audit after many findings is to follow up on the status of all recommendations, as this will ensure that the audit findings are addressed in a timely and effective manner, and that the root causes of the issues are resolved12. Following up on the status of all recommendations will also help to assess the

progress and performance of the IT department, and to identify any new or emerging risks or challenges34.

References

1: What to consider when resolving internal audit findings3 2: A brief guide to follow up4 3: Guidance on auditing planning for Internal Audit2 4: Corrective Action Plan (CAP): How to Manage Audit Findings1

NEW QUESTION: 334

□□ □□ □□□ □□ □ □□ □□□□ □□□□ □ □□□ □□□□□?

A. □□□ □□□□□ □□□□ □□□ □□□ □□

B. □□ □□□ □□□ □□ □□□ □□

C. □□ □□□□ □□□□ □□ □□□ □ □□□ □□

D. □□□ □□□ □□ □ □□ □□

Answer: (SHOW ANSWER)

The impact if corrective actions are not taken is the most important factor to consider when scheduling follow- up audits. An IS auditor should prioritize the follow-up audits based on the risk and potential consequences of not addressing the audit findings and recommendations. The other options are less important factors that may affect the timing and scope of the follow-up audits, but not their necessity or urgency. References:

* CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
* CISA Review Questions, Answers & Explanations Database, Question ID 207

NEW QUESTION: 335

□□ □ □□□□□ □□ □□□ □□□□?

A. □□□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□ □ □□□□□.

B. □□□ □□□ □□□ □□□□ □□ IP □□□ □□□□□ □□□□□ □□□□□□□.

C. □□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□□ □□□□ □□ □□□□ □ □□□□□.

D. □□□□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□□ □3□□□ □□□ □□.

Answer: B (LEAVE A REPLY)

An employee is induced to reveal confidential IP addresses and passwords by answering questions over the phone. This is a social engineering attack method that exploits the trust or curiosity of the employee to obtain sensitive information that can be used to access or compromise the network. According to the web search results, social engineering is a technique that uses psychological manipulationto trick users into making security mistakes or giving away sensitive information1. Phishing, whaling, baiting, and pretexting are some of the common forms of social engineering attacks2. Social engineering attacks are often more effective and profitable than purely technical attacks, as they rely on human error rather than system vulnerabilities

NEW QUESTION: 336
□□ □ □□ □□□(IoT) □□□ □□ □□ □□□□ □□□□ □□ IS □□□□ □□□□ □□ □□ □□□ □□□□□?
A. IoT □□□ □□ □□□ □□ □□□ □□□□□□ □□□.
B. IoT □□□ □□ □□□ □□ □□□□ □□□□ □□□.
C. IoT □□□ □□□ □□□□□□□ □□□ □ □□□ □□□.
D. IoT □□□□ □□ □ □□□ □□□□ □□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 337
□□□ □□ □□□□ □□ □□ □□(CSA) □□□□□ □□□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□□ □□□□. □□ □ □ □□ □□□ □□ □□□ □□□ □□ □□□?
A. □□ □□ □□□ □□□□□.
B. □□□ □□□ □□□□□.
C. □□□□ □□ □□□ □ □□□ □ □□□□.
D. □□ □□□□ □□ □□□ □□□ □ □□ □□□□□□.
Answer: (SHOW ANSWER)
The most significant benefit of implementing a control self-assessment (CSA) program and leveraging the internal audit function to test its internal controls annually is that risks are detected earlier. A CSA program is a process that enables business owners and managers to assess and improve their own internal controls on a regular basis, without relying on external auditors or consultants. A CSA program can help identify and mitigate risks, enhance performance, increase accountability, and foster a culture of control within the organization. By leveraging the internal audit function to test its internal controls annually, a small business unit can also obtain independent assurance and validation of its CSA results, as well as recommendations for improvement. This approach can help reduce compliance costs, as external audits may be less frequent or extensive. However, this is not the most significant benefit, as compliance costs are only one aspect of the total cost of risk. Business owners can also focus more on their core roles, as they can delegate some of their control responsibilities to their staff or teams through CSA. However, this is not the most significant benefit, as business owners still need to oversee and monitor their CSA activities and results, and ensure that they align with their strategic objectives and priorities. Line management may also be more motivated to avoid control exceptions, as they are directly involved in assessing and improving their own controls through CSA. However, this is not the most significant benefit, as motivation alone may not be sufficient to ensure effective control design and operation. References: Info Technology & Systems Resources | COBIT, Risk, Governance
... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 338
□□ □□□ □□□ □□ IT □□ □□□ □□ □□□□ □□□□□□□ □□□□ □ □□□ □ □□ □□ □□□□ □□□□□. □ □□ □□□□ □□ □□□ □□□ □ □□□□ □ □ □ □□□ □□ □□ □□ □ □□ □□□□?
A. □□□ □□□□□ □□ □□□
B. □□ □□□□□ □□
C. □□ CPU □□□ □□
D. □ □□□ MTBF(□□ □□ □□)
Answer: C (LEAVE A REPLY)
When identifying which servers are no longer required, reviewing server CPU usage trends is the most helpful approach. Monitoring the CPU usage over time provides insights into how actively a server is being utilized.
Servers with consistently low CPU usage may be candidates for consolidation or decommissioning. By analyzing CPU utilization patterns, IT management can make informed decisions about which servers can be retired without impacting performance or availability1.
References:
1.
ISACA. "Technical Guide on IT Migration Audit."
1(http://kb.icai.org/pdfs/PDFFile5b278a12a66758.
27269499.pdf)
2. Zapier. "IT audit: The ultimate guide [with checklist]." 2(https://zapier.com/blog/it-audit/)
3. ISACA. "CISA Certification | Certified Information Systems Auditor."
3(https://www.isaca.org
/credentialing/cisa)

NEW QUESTION: 339
□□□ □□ □□ IT □□ □□□□□ □□□□ □ □□ □ □□ □□ □□□□ □□□?
A. □□ □□□□□□ □□
B. □□□□□□(EVA)
C. □□□ □□
D. □□ □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 340
IS □□□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ RACI □□□ □□□□ □□□□□. □□ □□ □□ □□ □ □□ □□ □ □□□ □□□□ □?
A. □□□
B. □□□ □□
C. □□□

D. □□□ □ □□

Answer: D (LEAVE A REPLY)

The role within the RACI chart that would provide information on who has oversight of staff performing a specific task is accountable. A RACI chart is a matrix that defines and assigns the roles and responsibilities of different stakeholders for a project, process, or activity. RACI stands for responsible, accountable, consulted, and informed. Accountable is the role that has the authority and oversight to approve or reject the work done by the responsible role. The other options are not the roles that provide information on who has oversight of staff performing a specific task, as they have different meanings and functions. Consulted is the role that provides input or advice to the responsible or accountable roles. Informed is the role that receives updates or reports from the responsible or accountable roles. Responsible is the role that performs or executes the work or task. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 341

IS □□□□ □□ □□□□ □□□□□ □□□□ □ □□ □□□□ □□□ □□□□□□.
□ □□□ □□□ □□□□□ □ □□ □□□□□ □□ □□ □□ □□□□□.
□ □□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□□□?

A. □□□□□ □□□□ □□ □□ □□□ □□□ □□□□□.

B. □□□ □□ □□ □□□□□ □□ □□□ □□□□□.

C. □□□□□ □□□□□ □□ □□□□ □□ □□□□.

D. □□ □□ □□ □□□ □□□□ □□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

The issue seems to stem from a breakdown in the workflow or process for handling assets that are due for destruction12. By examining the workflow, the IS auditor can identify where the process failed, such as why the vendor was not notified about the hard drives12. This could involve reviewing procedures for inventory management, communication with vendors, and tracking of assets due for destruction12. The findings can then be used to improve the workflow and prevent similar issues in the future12.

References:

How To Properly Destroy A Hard Drive - Tech News Today

How to safely and securely destroy hard disk data - iFixit

NEW QUESTION: 342

IS □□□□ □□□□ □□ □□□□ □□□ □□□ □□□□ □□□□. □□□ □□□□ □ □□□ □□□ □□□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□ □ □□ □□□□?

A. □□ □□□ □□

B. □□□ □□ □

C. □□ □□ □□

D. □□ □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 343
□□□ □□□ IT □□□□ □□□□ □□□□ □□□□ □□□□□ □□ □□ □□□□□?
A. □□□□ □□□ □□□□
B. □□ □□□□□ □□□□ □□□□□ □□
C. □□□□ □□ □□
D. □□□□□□□ □□ □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 344
□□ □ IT □□□□□□ □□ □□□ □□□□□?
A. IT □□ □□ □□ □□ □ □□
B. IT □□ □□ □□ □ □□
C. □□□ □□□□ □□□ □□□□ □□ □□□□ □□
D. □□ □□□ □□ □□□□□ □□ □ □□
Answer: A (LEAVE A REPLY)
This means that the IT steering committee is responsible for ensuring that the IT strategy aligns with and supports the business strategy, vision, and goals of the organization. The IT steering committee is also responsible for overseeing and approving major IT initiatives, projects, and investments, and allocating resources and priorities accordingly12.
Developing and assessing the IT security strategy (B) is not the main responsibility of the IT steering committee, but rather a specific aspect of the IT strategy that may be delegated to a subcommittee or a dedicated security function. The IT steering committee may provide guidance and oversight for the IT security strategy, but it is not directly involved in developing and assessing it12.
Implementing processes to integrate security with business objectives is not the main responsibility of the IT steering committee, but rather an operational task that may be performed by the IT management and staff. The IT steering committee may monitor and evaluate the effectiveness of the security processes, but it is not directly involved in implementing them12.
Developing and implementing the secure system development framework (D) is not the main responsibility of the IT steering committee, but rather a technical task that may be performed by the IT developers and engineers. The IT steering committee may approve and endorse the secure system development framework, but it is not directly involved in developing and implementing it12.

NEW QUESTION: 345
□□ □ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□□□□?
A. □□□□□ □□ □□□ □□□ □□□□□.
B. □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□□□.

C. □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□□.
D. □□ □□(QA) □□ □□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
The most important aspect of an application development acceptance test is that user management approves the test design before the test is started, as this ensures that the test objectives, criteria, and procedures are aligned with the user requirements and expectations. The programming team's involvement in the testing process, the testing of data files for valid information before conversion, and the quality assurance (QA) team' s charge of the testing process are also important, but they are not as critical as user management's approval of the test design. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.4.2

NEW QUESTION: 346
□□□ □□□□ □□□□ □ IS □□□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□ □□
B. □□□□□□ □□ □□□
C. □□□ □□
D. □□ □□□
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
When an employee exploits avulnerability, the most appropriate audit is aforensic audit, as it focuses on investigating and documenting security incidentsfor legal or disciplinary action.
* Option A (Incorrect):Acompliance auditensures adherence to policies but does not investigate incidents in detail.
* Option B (Incorrect):Application security testinghelps identify vulnerabilities but does not address employee misuse.
* Option C (Correct):Aforensic auditgathersdigital evidence, determines how the exploit occurred, and ensures legal compliance in the investigation.
* Option D (Incorrect):Penetration testingidentifies weaknesses but does notanalyze past incidents.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Covers forensic investigations, digital evidence collection, and security incident response.

NEW QUESTION: 347
□□□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□□ □□ □□□ □□□□ IS □□□□□ □□ □□□ □□□ □□□□□?
A. □□ □ □□
B. □□ □ □□
C. □□ □□□ □□
D. □□□ □□□ □□
Answer: A (LEAVE A REPLY)
The condition that would be of most concern to an IS auditor assessing the risk of a successful brute force attack against encrypted data at rest is short key length. A brute force attack is a method of breaking encryption by trying all possible combinations of keys until finding the correct one. The shorter the key length, the easier it is for an attacker to guess or crack the encryption. Random key generation, use of symmetric encryption, and use of asymmetric encryption are not conditions that would increase the risk of a successful brute force attack. In fact, random key generation can enhance security by preventing predictable patterns in key selection. Symmetric encryption and asymmetric encryption are different types of encryption that have their own advantages and disadvantages, but neither is inherently more vulnerable to brute force attacks than the other. References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION: 348
IS □□□□ □□□□□ □□ □□(CRM) □□□ □□□□□□ □□□□□ □□ □□□□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□□□□□ 5□ □□□□ □□ □□□ □□□ □□□ □□□ □□□□□.
B. □□□□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□ □□□□ □□ □□□□ □□□□.
C. □□□ □□□□□□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □□ □ □ □□□.
D. □□ □□ □□□ □□□□ □□□ □□ □□□□ □□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 349
□□ □□□□ □□□ □□□□ IS □□□□ □□ □ □□□ □□□ □□□□□□□. □□ □ □□□ □□ □ □□□ □□ □□□□ □□ □□ □□□□□?
A. □□□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□ □□□□.
B. □□ □□□ □□□□ □□ □□ □□ □□□□□□.

C. □□□□ □□□ IT □□□□ □□□□□ □□□ □□□ □□□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□□□□ □□□□.
Answer: (SHOW ANSWER)
The performance and reliability of a job scheduling tool can be significantly affected if maintenance patches and the latest enhancement upgrades are missing1. These patches and upgrades often contain fixes for known issues and improvements to the tool's functionality. If they are not applied, the tool may continue to exhibit known problems or fail to benefit from enhancements that could improve its performance and reliability1. While factors like administrator password requirements23, number of support staff45, and tool classification64 can impact various aspects of a tool's operation, they are less likely to be the direct cause of performance and reliability problems.
References:
Patch Management Definition & Best Practices - Rapid7
Password must meet complexity requirements - Windows Security
NIST's New Password Rule Book: Updated Guidelines Offer Benefits and Risk - ISACA
Workforce optimization: Staff scheduling with AI | McKinsey Poor Employee Scheduling - Major Consequences And Solutions A Critical Analysis of Job Shop Scheduling in Context of Industry 4.0

NEW QUESTION: 350
□□ □ □□ □□ □□□ □□□□ □□□ □□□□ □□□□ □□ □□ □ □□□□?
A. SQL □□ □□
B. □□□ □□(DoS) □□
C. □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
A network firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A network firewall can help reduce the risk of denial of service (DoS) attacks, which are attempts to overwhelm a system or network with excessive requests or traffic, by filtering or blocking unwanted or malicious packets. A SQL injection attack is a type of code injection attack that exploits a vulnerability in a web application's database query, by inserting malicious SQL statements into the input fields. A phishing attack is a type of social engineering attack that attempts to trick users into revealing sensitive information or installing malware, by sending fraudulent emails or messages that impersonate legitimate entities. An insider attack is a type of malicious activity that originates from within an organization, such as employees, contractors, or partners, who abuse their access privileges or credentials to compromise the confidentiality, integrity, or availability of information systems or data. A network firewall cannot prevent these types of attacks, as they rely on exploiting human or application weaknesses rather than network vulnerabilities.

NEW QUESTION: 351
□□□ □□□ □□□ □□□ □□ □□□□ □□□□ □□□ □□ □ □□□□ □□ □□ □□□ □□□□□. □□ □□□ □□ □ IS □□□□ □□□□ □□□□ □□ □□□□□ □ □□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□□ □□□
B. □□□ □□□
C. □□ □□□
D. □□ □□□
Answer: C (LEAVE A REPLY)
Attribute sampling is a method of audit sampling that is used to test the effectiveness of controls by measuring the rate of deviation from a prescribed procedure or attribute. Attribute sampling is suitable for testing compliance with the data center's physical access log system, as the auditor can compare the identification document numbers and photos of the visitors with the records in the system and determine whether there are any discrepancies or errors. Attribute sampling can also provide an estimate of the deviation rate in the population and allow the auditor to draw a conclusion about the operating effectiveness of the control.
Variable sampling, on the other hand, is a method of audit sampling that is used to estimate the amount or value of a population by measuring a characteristic of interest, such as monetary value, quantity, or size.
Variable sampling is not appropriate for testing compliance with the data center's physical access log system, as the auditor is not interested in estimating the value of the population, but rather in testing whether the system is operating as intended.
Quota sampling and haphazard sampling are both examples of non-statistical sampling methods that do not use probability theory to select a sample. Quota sampling involves selecting a sample based on certain criteria or quotas, such as age, gender, or location. Haphazard sampling involves selecting a sample without any specific plan or method. Both methods are not suitable for testing compliance with the data center's physical access log system, as they do not ensure that the sample is representative of the population and do not allow the auditor to measure the sampling risk or project the results to the population.
Therefore, attribute sampling is the most useful sampling method for an IS auditor conducting compliance testing for the effectiveness of the data center's physical access log system.
References:
* Audit Sampling - What Is It, Methods, Example, Advantage, Reason
* ISA 530: Audit sampling | ICAEW

NEW QUESTION: 352
□□□ □□ □□ □□□ □□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□ □□
B. □□ □□

C. □□□ □□
D. □□□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 353
□□□ □□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□□□?
A. □□□ □□□□ □□□ □□ □□□ □□□□□ □□
B. □□□□ □ □□□□ □□ □□□ □□□ □ □□ □□□ □ □□□□□□.
C. □□ □□□ □□□□ □□ □□□ □□ □□□ □□ □□
D. □□□ □□□□ □□ □□ □□□ □□□□□ □□
Answer: D (LEAVE A REPLY)
Parallel processing is a system implementation approach that involves running the new system and the old system simultaneously for a period of time until the new system is verified and accepted. The primary advantage of parallel processing is that it provides assurance that the new system meets performance requirements and produces the same or better results as the old system. Parallel processing also minimizes the risk of system failure and data loss, as the old system can be used as a backup or fallback option in case of any problems with the new system.

NEW QUESTION: 354
□□ □□□ □□□(EUC) □□□ □□□□□ □□□ □□□ □□ □□□ □□□□ □□□.
A. EUC □□□ □□□□□□□.
B. EUC □□ □□□ □□□□ □□□□□□.
C. EUC □□□ □□□□□□□.
D. □□ □□ □□(BIA)□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 355
□□ □□ IT □□□□□□□ □□□ □, □□□ □□ □□ □□(SDLC)□ □□ □□□□ □ □□ □□□□ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□□ □□ □ □□□□
B. □□□□□ □□ □ □□
C. □□□ □□ □□□(UAT)
D. □□□□ □□
Answer: D (LEAVE A REPLY)
The most beneficial stage of the system development life cycle (SDLC) to consider data privacy principles is D: Requirements definition. This is because data privacy principles should be integrated into the design and development of customer-facing IT applications from the very beginning, not as an afterthought or a retrofit1. By considering data privacy principles in the requirements definition stage, the developers can identify the personal data that will be collected, processed, stored, and shared by the application, and ensure

that they comply with the relevant laws and regulations, such as the General Data Protection Regulation (GDPR)2. They can also apply the principles of data minimization, purpose limitation, transparency, consent, and security to protect the privacy rights and interests of the customers3.

NEW QUESTION: 356
□ □□□□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□ □ □□□ □□□
B. □□ □□ □□ □ □□ □□□□ □□
C. □□ □□□□ □□ □□
D. □□ □□ □□□ □□
Answer: (SHOW ANSWER)
The primary concern when negotiating a contract for a hot site is the availability of the site in the event of multiple disaster declarations. A hot site is a fully equipped alternative facility that can be used to resume business operations in the event of a disaster. However, if multiple clients of the hot site provider declare a disaster at the same time, there may be a shortage of resources or capacity to accommodate all of them. Therefore, the contract should specify the terms and conditions for ensuring the availability and priority of the hot site for the organization. The other options are not as important as availability, as they do not affect the ability to use the hot site in a disaster situation. Coordination with the site staff in the event of multiple disaster declarations is a logistical issue that can be resolved by communication and planning. Reciprocal agreements with other organizations are alternative arrangements that can be used to share resources or facilities in a disaster, but they may not be as reliable or suitable as a hot site. Complete testing of the recovery plan is a good practice that can help validate and improve the effectiveness of the recovery plan, but it is not a concern for negotiating a contract for a hot site. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3

NEW QUESTION: 357
□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□, □□□ □□□□□□ □□□□ □ □ IS □□□□ □□ □ □□ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□ □□□ □□□□□.
B. □□ □□□□ □□□□□.
C. □□□□□(DMZ)□ □□□□□.
D. □□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
A demilitarized zone (DMZ) is a network segment that is separated from the internal network and the external network, such as the internet, by firewalls or other security devices. A DMZ provides an extra layer of security for the organization's internal network by isolating the servers and services that need to be accessible to external users, such as a file server, from the rest of the network. A DMZ also prevents external users from

accessing the internal network directly, as they have to go through two firewalls to reach it. Therefore, setting up a DMZ is an IS auditor's best recommendation to protect anorganization from attacks when its file server needs to be accessible to external users12.

The other possible options are:

* Enforce a secure tunnel connection: This means that the organization requires external users to establish a secure and encrypted connection, such as a virtual private network (VPN), to access its file server.

This can provide some level of security and privacy for the data transmission, but it does not protect the file server or the internal network from attacks if the connection is compromised or if the external users are malicious. Therefore, enforcing asecuretunnel connection is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users3.

* Enhance internal firewalls: This means that the organization improves the security and performance of its internal firewalls, which are devices that filter and control the network traffic between different segments of the network. This can provide some level of protection for the internal network from unauthorized or malicious access, but it does not protect the file server or the external network from attacks if the file server is exposed to the internet or if the external network is compromised. Therefore, enhancing internal firewalls is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users4.

* Implement a secure protocol: This means that the organization uses a secure and standardized protocol, such as Secure File Transfer Protocol (SFTP) or Secure Shell (SSH), to transfer files between its file server and external users. This can provide some level of security and integrity for the data transmission, but it does not protect the file server or the internal network from attacks if the protocol is exploited or if the external users are malicious. Therefore, implementing a secure protocol is not an IS auditor's best recommendation to protect an organization from attacks when its file server needs to be accessible to external users5. References: 1: What Is a DMZ Network and Why Would You Use It? | Fortinet 2: Demilitarised zone (DMZ) | Cyber.gov.au 3: What Is VPN Tunneling? | Fortinet 4: Firewall

- Wikipedia 5: Secure Shell - Wikipedia

NEW QUESTION: 358

□□ □□ □□ □□ □□□□ □□□□□ □□ □□□ □□ □□□□ □□□□□. □□ □ IS □□□□ □□□ □□ □□□ □□□□□?

A. □□ □□□□ □□ □□ □□□ □□□□□.

B. □□ □□□□□ □□□□ □□□ □□□□□.

C. □□ □□□□ □□□ □□□ □□□□□ □□□ □□□ □□□□□.

D. □□□ □□□□ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

The IS auditor's best course of action in this situation is to present observations for discussion only.
Observations are factual statements or findings that are based on the audit evidence collected and analyzed during the audit. Observations can be presented to management for discussion and feedback, but they should not be considered as final conclusions or recommendations until the audit is completed and the audit report is issued. The other options are not appropriate for presenting the findings to date, as they may compromise the audit quality or integrity. Reviewing working papers with the auditee is not advisable, as working papers are confidential documents that contain the auditor's notes, calculations, and opinions that may not be relevant or accurate for management's review. Requesting the auditee provide management responses is premature, as management responses should be obtained after the audit report is issued and the audit findings andrecommendations are finalized. Requesting management wait until a final report is ready for discussion is impractical, as management may have a legitimate interest or need to know the audit progress and results as soon as possible. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.3

NEW QUESTION: 359
IS □□□□ □□□□□□□ □□□ □□ □□□ □□□ □□□□ □□□□. □□ □ □□ □ □□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□□ □□□□□.
B. □□□ □□□ □□□ □□ □□□□□ 3□ □ □□□ □□□□□□□.
C. □□□ □□□ □□□ □□□ □□□□ □□□□□.
D. □□□ □□ □□□(UAT)□ □□□□ □□ □□□ □□□ □□□□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 360
IS □□□□ □□ □□□□□□ □□□□ □□□□ □□ RFP□ □□□ □□□□ □□□□.
□□□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□□□ □□□ □□ □□□ □□□□ □□□.
B. □□ □□ □□□ □□□ □□□□ □□□.
C. □□□ □□□□□ □□ □□□ □□ □□□ □□□ □□□.
D. □□□□ □□□ □□□□□ □□□□□ □□□□ □□□.
Answer: (SHOW ANSWER)
This is because audit trails are records of system activity and user actions that can provide evidence of the validity and integrity of transactions and data in a financial application system. Audit trails can help to ensure compliance with laws, regulations, policies, and standards, as well as to detect and prevent fraud, errors, or misuse of information. Audit trails can also facilitate auditing, monitoring, and evaluation of the financial application system's performance and controls1.

The application should meet the organization's requirements (A) is not the best answer, because it is a general and obvious criterion that applies to any application system acquisition, not a specific and important recommendation for a financial application system. The organization's requirementsshould be clearly defined and documented in the RFP, but they may not necessarily include audit trails as a design feature.
Potential suppliers should have experience in the relevant area is not the best answer, because it is a factor that affects the selection of the supplier, not the design of the financial application system. The experience and reputation of potential suppliers should be evaluated and verified during the RFP process, but they may not guarantee that the supplier will include audit trails in the design.
Vendor employee background checks should be conducted regularly (D) is not the best answer, because it is a measure that affects the security and trustworthiness of the vendor, not the design of the financial application system. Vendor employee background checks should be performed as part of the vendor management and due diligence process, but they may not ensure that the vendor will include audit trails in the design.

NEW QUESTION: 361
□□□□□ □□ □□□ ERP(Enterprise Resource Planning) □□□□ □□ □□□ □□□ □□ □□□□ □□□□. □□ □□(QA) □□ □ □□ □ □□ □□□□ □ □□□ □□□□ □□?
A. □□□□
B. □□
C. □□□□□
D. □□
Answer: A (LEAVE A REPLY)
Stress testing is a type of performance testing that evaluates how a system behaves under extreme load conditions, such as high user traffic, large data volumes, or limited resources. It is useful for identifying potential bottlenecks, errors, or failures that may affect the system's functionality or availability. Stress testing during the quality assurance (QA) phase would have identified the concern of users complaining that a newly released ERP system is functioning too slowly. The other options are not as relevant for this concern, as they relate to different aspects of testing, such as regression testing (verifying that existing functionality is not affected by new changes), interface testing (verifying that the system interacts correctly with other systems or components), or integration testing (verifying that the system works as a whole after combining different modules or units). References: CISA Review Manual (Digital Version), Domain 5: Protection of Information Assets, Section 5.4 Testing Techniques1

NEW QUESTION: 362
□□□□ □□□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□ □□□ □□ □ □□□ □ IS □□□□ □□□□ □ □□ □□□ □□□ □□ □ □□□□□?
A. □□□ □□□ □□□□□.
B. □□□□□ □□□□ □□□□ □□□□□.
C. □□ □□□ □□ □□ □□ □□□ □□□□□.
D. □□ □□□ □□□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
Benford's Law analyzes numerical data to detect anomalies based on the frequency distribution of leading digits. For it to be effective, the dataset must follow specific criteria, including consistency in measurement units. If transactions are in different currencies, the leading digits can vary due to currency conversion rates, invalidating the analysis.
* Double Integer Format (Option A): Benford's Law applies to any set of numerical data, not specifically double integers.
* Random Selection of Transactions (Option B): The data set must represent the entire population, not a random selection.
* Limiting Analysis to Standard Deviations (Option C): This is irrelevant to the application of Benford's Law.
Reference: ISACA CISA Review Manual, Job Practice Area 2: Information Systems Audit and Assurance.

NEW QUESTION: 363
□□ □ □□ □□□□□□□ □□ □□□□ □□ □□ □□□ □ □□ □□ □□□ □□□ □ □□ □□□□□?
A. □□□□ □□
B. □□□ □□□
C. □□ □□ □□□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
Substantive testing provides the most reliable audit evidence on the validity of transactions in a financial application. Substantive testing is an audit procedure that examines the financial statements and supporting documentation to see if they contain errors or misstatements. Substantive testing can help to verify that the transactions recorded in the financial application are authorized, complete, accurate, and properly classified.

Substantive testing can include methods such as vouching, confirmation, analytical procedures, or physical examination.

NEW QUESTION: 364
□□□ □□ □□□□ □□□□ AI □□□□□ □□□□ □□□ □□□□ □ □□ □□ □ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□ □ AI □□□□ □□□□ □□ □□□
B. □□□ □□□ □□□□ □□□□□ □□□ □□
C. □□□ □□ □ □□□ □□ □□ □□
D. AI □□□□ □□□ □□□ □□□□
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Data collection and obtaining consentis themost critical regulatory requirementwhen using customer data for AI training, especially under laws likeGDPR, CCPA, and ISO 27701.
* Collection of Data and Obtaining Consent (Correct Answer - C)
* Ensures compliance withprivacy lawsthat require explicit customer consent.
* Example:UnderGDPR, companies mustinform usershow their data will be used and allow them toopt out.
* AI Algorithm Accuracy (Incorrect - A)
* Important formodel performancebutnot a primary legal concern.
* Ethical Use of Computing Resources (Incorrect - B)
* Ethical considerations are valuable butnot a regulatory priority.
* Continuous Monitoring of AI (Incorrect - D)
* Ensuresperformance, butregulatory compliance focuses on data privacy.
References:
* ISACA CISA Review Manual
* GDPR & CCPA Compliance Guidelines
* ISO 27701 (Privacy Information Management System)

NEW QUESTION: 365
IS □□□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□□.
□□□□ □□□ □□ □□ □□□□ □□□?
A. □□□ □□□ □□□ □□□□ □□□□□.
B. □□□□ □□□□ □□ □□ □□□□ □□□□□.
C. □□□ □□□□□.
D. □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The first step in addressing a vulnerability is to evaluate the associated risk, which involves assessing the likelihood and impact of a potential exploit. Based on the risk assessment, the appropriate mitigation strategy can be determined, such as implementing a new

system, addingfirewalls, or decommissioning the server. References: ISACA CISA Review Manual 27th Edition, page 280

NEW QUESTION: 366
□ □□□ □□ □□□□□□□ □ □□ □□□ □□□□ □□□□ □□ □□□ □□ □□ □□ □□□□□ □□□□□□. □□ □□□ □□□□ □□□ □□□ □□□ □□□ □□ □ □□□□□□?
A. □□□□□□ □□□□□□(DBaaS)
B. □□□□□□ □□□(IaaS)
C. □□□□□□ □□□(PaaS)
D. □□□□□□ □□□□□(SaaS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 367
IS □□□□ □□ □□□□□ □□□□□ □□□□ □□ □□□ □□□ □□□□.
A. □□ □□□ □□ □□□□ □□ □□□□□.
B. □□ □□ □□□ □□□□ □□ □ □□□.
C. □□ □□□ □□□ □□□□ □□ □□.
D. □□ □□ □□□ □□ □□.
Answer: (SHOW ANSWER)
The charging method for IS resources is the way that the IS function allocates its costs to the users or business units that consume its services. The charging method can affect the behavior and incentives of the users and the IS function, as well as the efficiency and effectiveness of the IS resources. Therefore, choosing an appropriate charging method is an important decision for the IS function and its stakeholders.
One of the possible charging methods is to charge specific costs that can be tied back to specific usage. This means that the IS function tracks and measures the actual consumption of each user or business unit for each IS service, and charges them accordingly. For example, if a user uses 10 GB of storage space, 5 hours of CPU time, and 100 MB of network bandwidth, the IS function will charge them based on the unit costs of these resources. This charging method has the advantage of encouraging the most efficient use of IS resources, as it provides clear and accurate feedback to the users about their consumption and costs, and motivates them to optimize their usage and avoid waste or overuse. This charging method also aligns the interests of the IS function and the users, as both parties benefit from reducing costs and improving efficiency.
The other possible charging methods are:
* Total utilization to achieve full operating capacity: This means that the IS function charges a fixed amount to each user or business unit based on their proportion of the total operating capacity of the IS resources. For example, if a user or business unit has 10% of the total computing power allocated to them, they will pay 10% of the total IS costs. This charging method has the disadvantage of discouraging efficient use of IS resources, as it

does not reflect the actual consumption or usage of each user or business unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates a mismatch between the interests of the IS function and the users, as the IS function benefits from increasing costs and capacity, while the users bear the burden of paying for them.
* Residual income in excess of actual incurred costs: This means that the IS function charges a markup or profit margin on top of its actual incurred costs to each user or business unit. For example, if a user or business unit consumes $100 worth of IS resources, the IS function will charge them $120, where $20 is the residual income for the IS function. This charging method has the disadvantage of discouraging efficient use of IS resources, as it increases the costs for the users and reduces their value for money. This charging method also creates a conflict between the interests of the IS function and the users, as the IS function benefits from increasing costs and profits, while the users suffer from paying more than they should.
* Allocations based on the ability to absorb charges: This means that the IS function charges different amounts to different users or business units based on their ability to pay or their profitability. For example, if a user or business unit is more profitable or has a higher budget than another user or business unit, they will pay more for the same amount of IS resources. This charging method has the disadvantage of discouraging efficient use of IS resources, as it does not reflect the actual consumption or usage of each user or business unit, and does not provide any incentive to reduce costs or improve efficiency. This charging method also creates an unfair and arbitrary distribution of costs among the users or business units, as some pay more than others for no valid reason. References: 1: Charging Methods for IT Services - IT Process Wiki 2: IT Chargeback Methods - CIO Wiki 3: IT Chargeback - Wikipedia

NEW QUESTION: 368
□□ □□□ □□□□ □□ □□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □ □□ □□□. □□ □ IS □□□□□ □□ □□□ □□□ □□□□□?
A. □□ □□□□ □□□ □□□□ □□ □□□□ □□□□□.
B. □□ □ □□□ □□□□ □□ □3□ □□□□□ □□□ □□ □□□□□.
C. □□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.
D. □□□□□□ □□□ □□□□ □□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
Collaborative discussions help address the auditee's concerns, find mutually agreeable solutions, and create buy-in for implementing improvements.
References
ISACA CISA Review Manual (Current Edition) - Chapters on audit reporting and communication Auditing Standards - Emphasize the importance of understanding and addressing auditee concerns.

NEW QUESTION: 369
□□ □ □□□ □□ □□□ □□□ □□ □ □□□ □□□□□?
A. □□□□ □□ □□□ □□□ □ □□□□.
B. □□□□□ □□□ □□ □□□ □□□ □ □□□□.
C. □□ □□□□□ □□□□ □□□ □ □□□□.
D. □□□□ □□□ □□□ □□□□ □□ □□ □□□ □ □ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 370
□□ □ □□□ □□ □□□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□□
B. □□□
C. □□□□□(CO2)
D. □□ □□□
Answer: (SHOW ANSWER)
The most appropriate and effective fire suppression method for an un-staffed computer room is carbon dioxide (CO2). Carbon dioxide is a gaseous clean agent that extinguishes fire by displacing oxygen and reducing the combustion process. Carbon dioxide is suitable for un-staffed computer rooms because it does not leave any residue, damage, or corrosion on the electronic equipment, and it does not require water or other chemicals that could harm the environment or human health. However, carbon dioxide can pose a risk of asphyxiation to any person who may enter the computer room during or after the discharge, so proper safety precautions and warning signs should be in place.
The other options are not as appropriate or effective as carbon dioxide for an un-staffed computer room:
* Water sprinkler. This is a common fire suppression method that uses water to cool down and extinguish fire. However, water sprinkler is not suitable for un-staffed computer rooms because it can cause severe damage to the electronic equipment, such as short circuits, corrosion, or data loss. Water sprinkler can also create a risk of electric shock to any person who may enter the computer room during or after the discharge.
* Fire extinguishers. These are portable devices that contain a pressurized agent that can be sprayed on a fire to put it out. However, fire extinguishers are not effective for un-staffed computer rooms because they require manual operation by a trained person who can identify the type and location of the fire, and use the appropriate extinguisher. Fire extinguishers can also cause damage to the electronic equipment if they contain water or chemical agents.
* Dry pipe. This is a type of sprinkler system that uses pressurized air or nitrogen in the pipes instead of water until a fire is detected. When a fire is detected, the air or nitrogen is released and water flows into the pipes and sprinklers. However, dry pipe is not ideal for un-staffed computer rooms because it still uses water as the extinguishing agent, which can damage the electronic equipment as mentioned above.

Dry pipe also has a slower response time than wet pipe sprinkler systems, which can allow the fire to spread more quickly.

NEW QUESTION: 371
□□□ □□□□□ □□□ □□ □□□□□ □□ □□ □□ □□ □□□ □□□□ IS □□ □□□ □□ □ □□□□ □□ □ □□□□□?
A. □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□.
B. □□□□□□□ □□□□□□□ □□□□ □□□□□.
C. □□ □□ □□□ □□ □□ □□(NDA)□ □□□□ □□ □□ □□□□□ □□□□□□ □.
D. □□□ □□ □□ □□□ □□ □□ □□(MTBF) □□□□□ □□□□ □□□.
Answer: (SHOW ANSWER)
The answer C is correct because preventive maintenance is outsourced to multiple vendors without requiring nondisclosure agreements (NDAs) would be of greatest concern to an IS auditor reviewing on-site preventive maintenance for an organization's business-critical server hardware. This is because outsourcing preventive maintenance to multiple vendors without NDAs exposes the organization to the risk of unauthorized access, disclosure, or modification of sensitive data and information stored on the servers. NDAs are legal contracts that bind the vendors to protect the confidentiality and security of the data and information they access or handle during the preventive maintenance. Without NDAs, the vendors may not have any obligation or incentive to safeguard the data and information, and they may misuse, leak, or compromise them for malicious or commercial purposes. This could result in financial losses, reputational damage, legal liabilities, or regulatory penalties for the organization.
The other options are not as concerning as option C. Preventive maintenance costs exceed the business allocated budget (option A) is a financial issue that may affect the profitability or efficiency of the organization, but it does not directly impact the security or availability of the server hardware. Preventive maintenance has not been approved by the information system (option B) is a procedural issue that may indicate a lack of coordination or communication between the IT department and the business units, but it does not necessarily affect the quality or effectiveness of the preventive maintenance. The preventive maintenance schedule is based on mean time between failures (MTBF) parameters (option D) is a technical issue that may influence the frequency or timing of the preventive maintenance, but it does not imply any risk or deficiency in the preventive maintenance itself.
References:
* What is a Maintenance Audit?
* How to audit your preventative maintenance schedule
* 5 Step Maintenance Management Program Audit
* How do you get effective Preventive Maintenance really?
* What is a Planned Preventative Maintenance Audit?

NEW QUESTION: 372
□□ □ □□ □□□□ □□□ □□□□□ □□□□ □□ □ □□□ □□□□□?
A. □□ □□□□□ □□□□□ □□□□□ □ □□□□.
B. TCP/IP(□□ □□ □□□□/□□□ □□□□)□ □□ □ □□ □□□ □□ □□□ □□□ □□.
C. □□ □□□ □□□ □□ □□□ □□□ □ □□□□.
D. □□□ □□□ □□□ □□□ □□□□□□ □□□□□□□□ □ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 373
□□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□□□
C. □□□ □□ □□
D. □□□□□ □□□□
Answer: (SHOW ANSWER)
The most important consideration when defining an operational log management strategy is understanding and meeting stakeholder requirements. This ensures that the strategy aligns with organizational needs and regulatory requirements, providing relevant and actionable information for security and compliance.
References
* ISACA CISA Review Manual 27th Edition, Page 273-274 (Log Management)

NEW QUESTION: 374
□□□ □□□□□ □□□ □□□□ □□□ □□ □□□ □□□□□ □ □ □□ □□ □□ □ □□ □□□ □□ □□□□□?
A. □□ □□
B. □□□□ □□□
C. □□□ □□□
D. □□
Answer: D (LEAVE A REPLY)
The most useful analytical method when trying to identify groups with similar behavior or characteristics in a large population is classification. Classification is a technique that assigns data points to predefined categories or classes based on their features or attributes. Classification can help to discover patterns, trends, and relationships among the data and reveal the similarities or differences among the groups. Classification can also help to support decision making, prediction, or recommendation based on the data analysis. References:
* CISA Review Manual (Digital Version), Chapter 3, Section 3.4.21
* CISA Online Review Course, Domain 2, Module 3, Lesson 12

NEW QUESTION: 375
□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□□□.
□□ □ IS □□□□ □□□ □□□ □□□ □□□ □ □□ □□□ □ □□ □□□□□?
A. □□ □ □□□ □□□ □□□□ □ □□
B. □□□□ □ □□□ □□□□ □□ □□
C. □□□ □□□□ □□ □□
D. □□□□ □□ □□ □□
Answer: B (LEAVE A REPLY)
The best way to evaluate the effectiveness of a new automated control is to review the written procedures that define the processes and controls. This will help the IS auditor to understand the objectives, scope, roles, responsibilities, and expected outcomes of the control. The written procedures will also provide a basis for testing the control and verifying its compliance with the audit finding recommendations. References:
* ISACA Frameworks: Blueprints for Success
* CISA Review Manual (Digital Version)

NEW QUESTION: 376
□□ □□ IS □□□□ □□ □□□□ □□□□ □□□ □□ □ □□□□□□ □□□□ □ □ □□□□□□□ □□□□ □□□□ □ □□□ □□ □□□□□□. □□ □ □□□□ □ □ □□□□ □□□□ □□ □□ □□□□ □□ □□□□□?
A. □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□.
B. □□ □□□ □□□ □□□□□□□.
C. □□ □□ □□□(IDS)□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 377
□□ □ □□ □□ □□□ □□□ □□□ □□□□□?
A. □□□ □□□ □□ □ □□
B. □□□ □□ □□
C. □□□□□ □□□ □□
D. □□□ □□□ □□ □ □□

Answer: C (LEAVE A REPLY)
Data integrity is the property that ensures that data is accurate, complete, consistent, and reliable throughout its lifecycle. The best data integrity check is tracing data back to the point of origin, which is the source where the data was originally created or captured. This check can verify that data has not been altered or corrupted during transmission, processing, or storage. It can also identify any errors or discrepancies in data entry or conversion. Counting the transactions processed per day is a performance measure that does not directly assess data integrity. Performing a sequence check is a validity check that ensures that data follows a predefined order or pattern. It can detect missing or out-of-order data elements, but it cannot verify their accuracy or completeness. Preparing and running test data is a testing technique that simulates real data to evaluate how a system handles different scenarios. It can help identify errors or bugs in the system logic or functionality, but it cannot ensure data integrity in production environments. References: Information Systems Operations and Business Resilience, CISA Review Manual (Digital Version)

NEW QUESTION: 378
□□□□□ □□ □□□□□ □□ □□□□ IS □□□□ □□ □□□ □□□ □□□□ □□ □□.
A. □□ □□□□□ □□ □□□.
B. □□ □□□□□ □□□ □□.
C. □□□ □□□ □□□ □□ □□.
D. □□ □□□□ □□□.
Answer: C (LEAVE A REPLY)
The primary responsibility of an IS auditor during the design phase of a software development project is to evaluate the controls incorporated into the system specifications. Controls are mechanisms or procedures that aim to ensure the security, reliability, or performance of a system or process. System specifications are documents that define and describe the requirements, features, functions, or components of a system or software. Evaluating the controls incorporated into the system specifications is a key responsibility of an IS auditor during the design phase of a software development project, as it helps ensure that the system or software meets the organization's objectives, standards, and expectations for security, reliability, or performance. The other options are not primary responsibilities of an IS auditor during the design phase of a software development project, as they do not directly relate to evaluating the controls incorporated into the system specifications. Future compatibility of the application is a possible factor that may affect the functionality or usability of the application in different environments or platforms, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. Proposed functionality of the application is a possible factor that may affect the suitability or value of the application for meeting user needs or expectations, but it is not a primary responsibility of an IS auditor during the design phase of a software

development project. Development methodology employed is a possible factor that may affect the quality or consistency of the software development process, but it is not a primary responsibility of an IS auditor during the design phase of a software development project. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 379

□□ □□□□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□ IS □□□□ □□ □□ □□□ □□ □□□?

A. □□□ □□□ □□□ □□□□ □□□□□.

B. □□□□□□ □□□□ □□□□□.

C. □□ □□□ □□□□□ □□□ □□□□□ □□□□□.

D. □□ □□□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

The first thing that an IS auditor should do when a follow-up audit reveals some management action plans have not been initiated is to escalate the lack of plan completion to executive management. This is because the failure to implement the agreed management action plans may indicate that the management is not taking the audit findings and recommendations seriously, or that they are accepting too much risk by not addressing the identified issues. Escalating the lack of plan completion to executive management can help to raise awareness and accountability, as well as to seek support and intervention to ensure that the management action plans are executed in a timely and effective manner12.

Confirming whether the identified risks are still valid is not the first thing to do, although it may be a useful step to reassess the current situation and the potential impact of not implementing the management action plans. However, confirming the validity of the risks does not address the root cause of why the management action plans have not been initiated, nor does it provide any assurance or remediation for the unresolved issues34.

Providing a report to the audit committee is not the first thing to do, although it may be a necessary step to communicate and document the results of the follow-up audit. However, providing a report to the audit committee does not guarantee that the management action plans will be initiated, nor does it resolve any conflicts or challenges that may prevent the management from implementing them34.

Requesting an additional action plan review to confirm the findings is not the first thing to do, although it may be a prudent step to verify and validate the accuracy and completeness of the follow-up audit. However, requesting an additional review may delay or defer the implementation of the management action plans, as well as consume more internal audit resources and time

NEW QUESTION: 380

IS □□□□ □□□ □□□□ □□ □□□□□□ □□□(DBA)□ □□□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□□□□. □□□□ □□ □ □ □□ □□ □□□□ □□□?

A. □□ DBA□ □□□ □ □ □□□ □□□□□.

B. □□ □□ □□ □□□ □□

C. □□ □□□ □□□□□ □□□□□.

D. □□ □□ □□ □□ □□□□□ □□□□□□ □□□□□.

Answer: (SHOW ANSWER)

A database administrator (DBA) is responsible for maintaining the integrity, security and performance of the database systems. A DBA who is also responsible for developing and executing changes into the production environment may have a conflict of interest and pose a risk to the data quality and availability. Therefore, the IS auditor should first identify whether any compensating controls exist to mitigate this risk, such as independent reviews, approvals, audits or monitoring of the changes. Determining whether another DBA could make the changes, reporting a potential segregation of duties violation and ensuring a change management process is followed prior to implementation are possible actions that the auditor could take after identifying the compensating controls or the lack thereof.

References:

* : Database Administrator (DBA) Definition
* : Segregation of Duties | ISACA
* : [Compensating Control Definition]

NEW QUESTION: 381

□□ □ □□□ □□□ □□□□ □□□ □□□ □□□ IT □□□□ □□□ □ □□ □□ □ □□ □□□□ □□□ □□□□□?

A. □□ □□ □□□(MTO)

B. □□ □□ □□(RPO)

C. □□□ □□ □□(SDO)

D. □□ □□□ □□ □(AIW)

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed In-Depth Explanation:Maximum Tolerable Outage (MTO) (A) defines the longest time an organization can tolerate an IT service being unavailable before significant business impact occurs. It determines business continuity planning and disaster recovery strategies.

Other options:

* RPO (B) defines acceptable data loss but does not determine the total outage limit.
* SDO (C) is related to service agreements but does not set the risk threshold.
* AIW (D) is similar to MTO but is not as commonly used in disaster recovery planning.

Reference: ISACA CISA Review Manual, Information Systems Operations and Business Resilience

NEW QUESTION: 382
□□□ □□□ □□□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□
C. □□ □□ □□ □□
D. □□□ □□(UAT) □□
Answer: D (LEAVE A REPLY)
When auditing the closing stages of a system development project, the most important consideration should be the user acceptance test (UAT) results. The UAT is a critical phase of the system development life cycle (SDLC) that ensures that the system meets the functional requirements and expectations of the end users. The UAT results provide evidence of the system's quality, performance, usability, and reliability. Control requirements, rollback procedures, and functional requirements documentation are also important considerations, but they are not ascrucial as the UAT results in determining if the system is ready for deployment. References: CISA Review Manual (Digital Version)1, page 325.

NEW QUESTION: 383
□□ □ □□□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □□ □□ □□ □ □□ □□□□□?
A. □□□ □□ □□□
B. CAAT□ □□ □□□□□
C. □□□□ □□□ □□□□ □□ □□□ □□□
D. □□ □□□□ □□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 384
□□ □□□ IS □□□□ □□ □□□ □□□□ □□ □□ □ □□□ □□□ □□□□□. □ □ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□ □□□□□.
B. □□□□□ 10% □□ □□ □□□ □□ □□□□□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□□ □□□□□.
D. □□ □□□□□ □□ □□□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
A post-implementation review (PIR) is a process to evaluate whetherthe objectives of the project were met, determine how effectively this wasachieved, learn lessons for the future, and ensure that the organisation gets the most benefit from the implementation of projects1. A PIR is an important tool for assessing the success and value of a project, as well as identifying the areas for improvement and best practices for future projects.
One of the key elements of a PIR is to measure the benefits of the project against the expected outcomes and benefits that were defined at the beginning of the project.

Measurable benefits are the quantifiable and verifiable results or outcomes that the project delivers to theorganisation or its stakeholders, such as increased revenue, reduced costs, improved quality, enhanced customer satisfaction, or compliance with regulations2. Measurable benefits should be aligned with the organisation's strategy, vision, and goals, and should be SMART (specific, measurable, achievable, relevant, and time-bound).
The finding that measurable benefits were not defined is of greatest significance among the four findings, because it implies that:
* The project did not have a clear and agreed-upon purpose, scope, objectives, and deliverables
* The project did not have a valid and realistic business case or justification for its initiation and implementation
* The project did not have a robust and effective monitoring and evaluation mechanism to track its progress, performance, and impact
* The project did not have a reliable and transparent way to demonstrate its value proposition and return on investment to the organisation or its stakeholders
* The project did not have a meaningful and actionable way to learn from its achievements and challenges, and to improve its processes and practices Therefore, an IS auditor should recommend that measurable benefits are defined for any project before its implementation, and that they are reviewed and reported regularly during and after the project's completion.
The other possible findings are:
* A lessons-learned session was never conducted: This is a significant finding, but not as significant as the lack of measurable benefits. A lessons-learned session is a process of capturing and documenting the knowledge, experience, and feedback gained from a project, both positive and negative. A lessons- learned session helps to identify the strengths and weaknesses of the project management process, as well as the best practices and lessons for future projects. A lessons-learned session should be conducted at the end of each project phase or milestone, as well as at the end of the project. However, even without a formal lessons-learned session, some learning may still occur informally or implicitly among the project team members or stakeholders.
* The projects 10% budget overrun was not reported to senior management: This is a significant finding, but not as significant as the lack of measurable benefits. A budget overrun is a situation where the actual cost of a project exceeds its planned or estimated cost. A budget overrun may indicate poor planning, estimation, or control of the project resources, or unexpected changes or risks that occurred during the project implementation. A budget overrun should be reported to senior management as soon as possible, along with the reasons for it and the corrective actions taken or proposed. However, a budget overrun may not necessarily affect the quality or value of the project deliverables or outcomes if they are still within acceptable standards or expectations.
* Monthly dashboards did not always contain deliverables: This is a significant finding, but not as significant as the lack of measurable benefits. A dashboard is a visual tool that

displays key performance indicators (KPIs) or metrics related to a project's progress, status, or results. A dashboard helps to monitor and communicate the performance of a project to various stakeholders in a concise and clear manner. A dashboard should include deliverables as one of its components, along with other elements such as schedule, budget, quality, risks, issues, or benefits. However, even without deliverables in monthly dashboards, some information about them may still be available from other sources such as reports or documents.
References: 1: What is Post-Implementation Review in Project Management? 2: The role & importance of the Post Implementation Review

NEW QUESTION: 385
□□□ □□□□ □□ □□□ □□□□□□□ □□ □□□□□ □□□□ □□□ □□□□ □□. □□□ □□□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□(IDS)□ □□□□□□
B. □□ □□□□□ □□□ □□□□□.
C. □□□ □□□ □□□ □□□ □□□□□.
D. □□□□ □□□□ □□□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
The primary purpose of creating a simulated production environment with multiple vulnerable applications is D: To attract attackers in order to study their behavior. This is also known as a honeypot, which is a decoy system that mimics a real target and lures attackers into revealing their techniques, tools, and motives1. A honeypot can help the organization's security team to improve their defense strategies, identify new threats, and collect digital evidence of cyberattacks1.

NEW QUESTION: 386
IS □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□□. □□ □ □□ □□□ □□ □ □□□□ □□ □□□ □□□□□?
A. □□□ □□□□□ □□ □□ □□□ □□□□□□□.
B. □□□□ □□□ □□□□ □□ □□□ □□ □□□□□.
C. □□ □□□□ □□□□ □ □□□□□ □□□□ □□□□□□□□ □□□□□.
D. □□□ □□□□ □□□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
The finding that presents the most significant risk when reviewing the deployment of a new automated system is that data from the legacy system is not migrated correctly to the new system. Data migration is a critical process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. If data migration is not performed correctly, it can result in data loss, corruption, inconsistency, or duplication, which can affect the functionality, performance, reliability, and security of the new system. Data migration errors can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The other findings

(A, B and D) are less significant risks, as they can be mitigated by rehiring or retraining personnel, providing user training, or adapting the system to different platforms.

NEW QUESTION: 387
□□ □ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□□.
B. □□ □□□ □□ □□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□□.
C. □□ □□□ □□ □□□□□ □□□ □□□ □□□ □□□□.
D. □□ □□□ □□ □□□ □□ □□ □□□ □ □□□□.
Answer: C (LEAVE A REPLY)
A contingency facility is a backup site that can be used to resume business operations in the event of a disaster or disruption at the primary site. The most important consideration for a contingency facility is that it is located a sufficient distance away from the primary site, so that it is not affected by the same event that caused the disruption. For example, if the primary site is damaged by a fire, flood, earthquake, or terrorist attack, the contingency facility should be in a different geographic area that is unlikely to experience the same hazard. This way, the organization can continue to provide its services and products to its customers and stakeholders without interruption.
The other options are not as important as the location of the contingency facility. The badge access controls, the number of business assets, and the identifiability of the sites are secondary factors that may affect the security and efficiency of the contingency facility, but they are not essential for its functionality. Therefore, option C is the correct answer.
References:
The Importance of Contingency Planning
WHO guidance for contingency planning

NEW QUESTION: 388
□□□□ □□ □□□ □□□ □□□□ □□□ □□□□□ □□□□□□. □□ □ IS □□ □□ □□ □□ □□□ □□□□□ □□□?
A. □□ □□□ □□ □□ □□□ □□□□□.
B. □□ □□□□ □□ □□ □□□ □□.
C. □□□□ □□□ □□□□□.
D. □□□□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 389
□□ □ □□ □□□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□□
B. □□□ □□ □□□□
C. □□□ □□
D. □□□ □□□

Answer: C (LEAVE A REPLY)
The most effective method of destroying sensitive data stored on electronic media is physical destruction, which involves breaking, shredding, melting, or incinerating the media to make it unreadable and unrecoverable. Degaussing, random character overwrite, and low-level formatting are methods of sanitizing or erasing data from electronic media, but they do not guarantee complete destruction of data and may leave some traces that can be recovered by advanced techniques. Therefore, physical destruction is the most secure and reliable method of data disposal for sensitive data. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Data Disposal

NEW QUESTION: 390
□□□□□ □□□ □□ □□□ □□□ □□□□ □□ □ □□□ □□□ □□□□.
A. □□□□ □□ □□□ □□□□□□.
B. □□□ □□□ □ □□□ □□□ □□□ □□□□.
C. □□□□□ □□□□□ □□□□ □□□.
D. □□ □□(QA) □□□□ □□□ □□
Answer: C (LEAVE A REPLY)
The greatest benefit of using a prototyping approach in software development is that it helps to conceptualize and clarify requirements. A prototyping approach is a method of creating a simplified or partial version of a software product to demonstrate its features and functionality. A prototyping approach can help to elicit, validate, and refine the requirements of the software product, as well as to obtain feedback from the users and stakeholders. The other options are not the greatest benefits of using a prototyping approach, but rather possible outcomes or advantages of doing so. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.3.11
* CISA Review Questions, Answers & Explanations Database, Question ID 227

NEW QUESTION: 391
□□ □ □□ □□□ □□□□ □□□□ □□□□ □□□□□□□□ □□□□ □□□□ □ □□ □□□□□?
A. □□□
B. □□
C. □□□□
D. □□
Answer: (SHOW ANSWER)
The best environment for copying data and transforming it into a compatible data warehouse format is the staging environment. The staging environment is a temporary area where data from various sources are extracted, transformed, and loaded (ETL) before being moved to the data warehouse. The staging environment allows for data cleansing, validation, integration, and standardization without affecting the source or target systems. The testing environment is not suitable for copying data and transforming it into a

compatible data warehouse format, as it is used for verifying and validating the functionality and performance of applications or systems. The replication environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating identical copies of data or systems for backup or recovery purposes. The development environment is not suitable for copying data and transforming it into a compatible data warehouse format, as it is used for creating or modifying applications or systems. References:
* CISA Review Manual, 27th Edition, pages 475-4761
* CISA Review Questions, Answers & Explanations Database, Question ID: 2642

NEW QUESTION: 392
□□ □ IT □□□□□ □□□□□□ □□ □□□ □□□ □ □□ □□□□□ □□□□ □□ □□ □□□□□?
A. □□ □□□ □□□
B. □□ □□ □ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 393
IS □□□□ □□ □□ □□□□□ □□□ □□□□□□ □□□□ □□ □□ □ □□ □□ □ □□ □□ □□□□□?
A. □□ □□□ □□□
B. □□□ □□□ □□
C. □□ □□ □□
D. □□ □□□ □□□□
Answer: (SHOW ANSWER)
Operating system parameters are settings or values that affect the behavior or performance of the operating system1. Modifications to the operating system parameters may be necessary to improve the system functionality, security, or efficiency. However, such modifications may also introduce risks or errors that can affect the system stability, compatibility, or integrity. Therefore, modifications to the operating system parameters should be authorized and documented by the appropriate authority2.

A change control log is a record of all changes made to the system, including the date, time, description, reason, authorization, and impact of each change3. A change control log can help the IS auditor to verify whether modifications to the operating system parameters were authorized by comparing the log entries with the actual system settings and the change approval documents4.

NEW QUESTION: 394
□□□ □□□□ □□ □□ □□□□ □□□□ □□□□□□ □□□ □□□ □□□□ □ □ □ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□□ □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
B. □□□ □□□ □ □□□□ □□□ □□□ □□□□□.
C. □□□ □□□ □□□ □□□ □□ □□□□□ □□□□□.
D. □□ □□□ □□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The most important consideration for patching mission critical business application servers against known vulnerabilities is A. Patches are implemented in a test environment prior to rollout into production. This is because patching mission critical business application servers involves a high level of risk and complexity, and requires careful planning and testing before applying the patches to the live environment. Patches may introduce new bugs, errors, or conflicts that could affect the functionality, performance, or security of the application servers, and cause system downtime, data loss, or business disruption1. Therefore, it is essential to implement patches in a test environment first, where the patches can be verified and validated for their effectiveness and compatibility, and any issues or defects can be identified and resolved before they impact the production environment2.

NEW QUESTION: 395
□□□ □□ □□□□ □□□□□ □□□ □□□□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□
B. □□□□
C. □□□ □□
D. □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 396
□□□ □□ □□□ □□□□ AI □□□ □□ □□□ □□□ □ IS □□□□ □□ □□ □□ □ □□□ □□□ □□□.
A. AI □□□□ □□ □□□□ □□□ □□.
B. AI □□□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□ □□□ □□□ □□□.

D. AI □□□□ □□ □□ □□□ □□□ □□□ □ □□ □□.

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

Theprimary concernwhen auditing an AI-powered chatbot is ensuring thesafeguarding of personal datato comply with privacy regulations such asGDPR, CCPA, and ISO 27701. AI chatbots process customer inquiries, often handling sensitive personal data.

* Safeguarding of Personal Data (Correct Answer - A)
* Ensures compliance with data protection laws.
* Reduces the risk of unauthorized access or data leakage.
* Example:An AI chatbot collecting customer financial information must follow encryption and access control policies.
* Compliance with Industry Standards (Incorrect - B)
* Important, but protecting customer data takes priority over general compliance.
* Speed and Accuracy of Chatbot Responses (Incorrect - C)
* A performance metric, but not a primary audit focus.
* AI's Ability to Handle Multiple Queries (Incorrect - D)
* Efficiency metric, but does not address security risks.

References:

* ISACA CISA Review Manual
* ISO 27701 (Privacy Information Management System)
* GDPR & CCPA Compliance Guidelines

NEW QUESTION: 397

□□ □□□ □□ □ □□ □□ □□□□□?

A. □□□□ □□

B. □□ □□ □□□

C. □□□ □□□

D. □□ □□ □□

Answer: D (LEAVE A REPLY)

Coding standards provide field naming conventions, which are rules for naming variables, constants, functions, classes, and other elements in a program. Coding standards help to ensure consistency, readability, maintainability, and portability of code. Program documentation, access control tables, and data flow diagrams are not part of coding standards. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

NEW QUESTION: 398

IS □□□□ □□ □□ □□ □ □□□□ □□□□□ □□ □□ □□□□ □□□ □□□ □ □□□ □□□ □□□ □□□□□ □□□ □□ □□□□. □□ □□ □□ □ □□ □□ □ □ □□ □□□□ □□□□ □□ □□□□?

A. □□ □□ □□□□□ □□□ □□ □□ □□

B. □□□□ □□□ □□ □□ □□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□ □.
C. □□ □□ □□□□ □□□ □□ □□ □□ □□
D. □□ □□ □□ □□□□ □□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
The audit procedure that would have most likely identified the exception of critical servers not included in the central log repository is to compare a list of all servers from the directory server against a list of all servers present in the central log repository. This would allow the IS auditor to detect any discrepancies or omissions in the central log repository. The other audit procedures (A, C and D) would not be effective in identifying this exception, as they would only focus on the alerts generated, the alert settings configured, or the servers included in the previous year's audit, which may not reflect the current state of the central log repository. References: IS Audit and Assurance Guideline 2202: Evidence Collection Techniques, CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.3: Logging and Monitoring

NEW QUESTION: 399
IS □□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□ □ □□□ □□□□. □□ □ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□ □□□
B. □□□ □□□
C. □□□□ □□□
D. □□ □□□
Answer: D (LEAVE A REPLY)
The best sampling method to use for verifying the adequacy of an organization's internal controls and being concerned about potential circumvention of regulations is B. Random sampling. Random sampling is a method of selecting a sample from a population in which each item has an equal and independent chance of being selected1. Random sampling reduces the risk of bias or manipulation in the sample selection, and ensures that the sample is representative of the population. Random sampling can be used for both attribute and variable sampling, which are two types of audit sampling that test for the occurrence rate or the monetary value of errors, respectively2.

NEW QUESTION: 400
□□ □ □□□ □□□□□ □□□□ □□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□ □□□□
B. Kerberos □□
C. □□ □□
D. □□□□(CA)
Answer: (SHOW ANSWER)

A certificate authority (CA) is critical in a public key cryptographic system for mitigating man-in-the-middle (MITM) attacks. It ensures that public keys are authentic by issuing digital certificates, which bind a public key to an entity. The CA's role in verifying identities and providing trust anchors prevents attackers from spoofing keys.
* Strong Encryption Algorithms (Option A):Encryption ensures confidentiality but does not address spoofing risks.
* Kerberos Authentication (Option B):Useful for mutual authentication but not central to public key infrastructure (PKI).
* Registration Authority (Option C):Supports the CA but does not directly prevent MITM attacks.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 401
□□ □ □□□ □□□□ □□□□ □□□□ □ □□ □□□ □□ □□□□□ □□□□ □ □ □□□□□?
A. □□□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 402
IS □□□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□ □□□□ □□□ □ □□ □□ □□□ □□ □□□ □□ □ □□□□□?
A. □□□ □□□□ □□ □□ □ □□ □□ □□
B. □ □□□□□ □□□ □□ □□ □□ □□ □□
C. □□ □□ □□ □□ □□ □ □□
D. □□ □□□ □□□□ □□
Answer: C (LEAVE A REPLY)
The best source of information for an IS auditor to use as a baseline to assess the adequacy of an organization' s privacy policy is the local privacy standards and regulations. Privacy standards and regulations are legal requirements that specify how personal data should be collected, processed, stored, shared, and disposed of by organizations. By using local privacy standards and regulations as a baseline, the IS auditor can ensure that the organization's privacy policy complies with the applicable laws and protects the rights and interests of data subjects. Historical privacy breaches and related root causes, globally accepted privacy best practices, and benchmark studies of similar organizations are useful sources of information for improving an organization's privacy policy, but they are not as authoritative and relevant as local privacy standards and

regulations. References: CISAReview Manual (Digital Version): Chapter 2 - Governance and Management of Information Technology

NEW QUESTION: 403
□□ □ □□ □□□ IT □□□□□□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □ □□□□?
A. □□ □□(QA) □□□
B. □□□□ □□□
C. □□□□ □□□
D. □□ □□ □□□(CRO)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 404
□□□□ □□□□ □□ □□□ □□□ □□□ □□□□□ □□□□□. □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□□ □□ □□□□□ □□□□
B. □□□□ □□ □□□ □□ □□ □□
C. □□□□ □□ □□□□□ □□□□ □□□□ □□
D. □□□□ □□ □□□□ □□□□ □□□ □□□□ □□ □□□□□.
Answer: B (LEAVE A REPLY)
Partitioning the work environment from personal space on devices. This would best maintain information security without compromising employee privacy by creating a separate and secure area on the personal mobile devices for work-related data and applications. This way, the organization can protect its information from unauthorized access, loss, or leakage, while respecting the employees' personal data and preferences on their own devices.
The other options are not as effective as option B in balancing information security and employee privacy.
Option A, installing security software on the devices, is a good practice but may not be sufficient to prevent data breaches or comply with regulatory requirements. Option C, preventing users from adding applications, is too restrictive and may interfere with the employees' personal use of their devices. Option D, restricting the use of devices for personal purposes during working hours, is impractical and difficult to enforce.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* Personal Cellphone Privacy at Work1
* Protecting your personal information and privacy on a company phone2
* Mobile Devices and Protected Health Information (PHI)3
* Using your personal phone for work? Here's how to separate your apps and data4

* 9 Ways to Improve Mobile Security and Privacy in the Age of Remote Work5

NEW QUESTION: 405
□□ □ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□□□?
A. □□□ □□□□□ 3□ □□□□ □□□ ID□ □□□□□.
B. □□□ □□ □□ □□ □□□ □□□□□.
C. □□□□ □□ □□ □□□□ □□ □□ □□□□ □□□□ □□□.
D. □□ □□□□ □□ □□ □□ □□(DRP)□ □□□□ □□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 406
□□ □□ □□□□ □□ □□ □□ IT □□□□ IS □□□□ □□□□□□□ □□ □□ □ □□ □□ □□□□□ □□□□□□ □□□ □□□ □□□□□□. □□ □ □□□□ □□□ □ □□ □□ □□□ □□□□□?
A. IT □□ □□□ □□□ □□□ □□ □□ □□ □□□ □□□□ □□□□□.
B. □□□□ IT □□□ □□□ □□□ □□ □□□ □□□□□.
C. IT □□□□ □□□ □□□ □□□ □□□ □□□□□.
D. □□□ □□□□ □□ □□□ □□ □□□□□.
Answer: (SHOW ANSWER)
The auditor's best action is to re-perform the audit before changing the conclusion, because the auditor needs to obtain sufficient and appropriate evidence to support the audit opinion. The evidence provided by IT management may not be reliable or relevant, and it may not reflect the actual effectiveness of the control during the audit period. Therefore, the auditor should verify the evidence independently and test the control again to ensure that it meets the audit criteria and objectives. The other options are not appropriate, because they either ignore or accept the evidence provided by IT management without verification, which may compromise the quality and integrity of the audit. References:
* ISACA, CISA Review Manual, 27th Edition, chapter 1, section 1.51
* ISACA, IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 12062

NEW QUESTION: 407

□□ □□ □□ □□□□ □□□ □□□ □□ □□ □□□□□ □□□□□□□. □□ □□ □□□ □□ □□□□ □□□□ □□ IS □□□□ □□ □ □□ □□ □□ □□□□ □□□ □□?

A. □□□ □□□□□ □□□□□□.

B. 2□□ □□ □□

C. □□□ □□ □□

D. □□□ □□□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

According to the CISA - Certified Information Systems Auditor Study Guide1, the correct answer to your question is A. Encrypt the disk drive. This is because encryption is a logical security measure that can protect data even if the physical device is stolen or lost. Encryption makes the data unreadable and inaccessible without the proper key or password. The other options are not as effective as encryption in this scenario. Two- factor authentication is a user authentication method that requires two pieces of evidence to verify the user's identity, such as a password and a code sent to a phone. However, this does not prevent unauthorized access to the data if the laptop is already logged in or if the attacker can bypass the authentication. Enhancing physical security is a preventive measure that can reduce the risk of theft, but it does not guarantee that theft will not occur or that the data will be safe if it does. Requiring the use of cable locks is another preventive measure that can deter thieves, but it can also be easily cut or removed by a determined attacker.

NEW QUESTION: 408

□□□□ □□□□□□□ □□□□□□□ □ □ □□ □□ □□□ □□□□□. □□ □ □ □ □□□□□ □□ □□ □□ □□□ □ □ □□□□□ □□□ □□ □□ □□□□?

A. □□□□ □□□ □□□ □□□ □□ □□□□ □□□□

B. □□□□□□ □□ □□□□ □□ □□

C. □□ □□□□ □□ □□ □□ □□

D. □□□□□□ □□ □□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 409

□□□ □□□ □□ □□ □□□ □□ □□□□□ □□□ □ □□ □□ □□□□ □ □□□ □□□□□?

A. □□ □□□ □□□ □□□ □□

B. □□□ □□ □□ □□ □□

C. □□□ □□□ □□□ □□

D. □□□ □ □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 410

IS □□□□ □□□ □□□ □□□□□ □□□□□ □□□□□□ □□□□ □□□ □□ □ □□□□. □□ □ □□ □□ □□□ □□□ □□□ □□□□□ □□□ □□□□ □ □□ □ □ □□□ □□□□□?

A. □□ □□

B. □□ □□

C. □□

D. □□ □□

Answer: A (LEAVE A REPLY)

The best evidence to determine whether transactions have been executed by authorized employees is audit trails. Audit trails are secure records that catalog events or procedures to provide support documentation. They are used to authenticate security and operational actions, mitigate challenges, or provide proof of compliance and operational integrity2.

Audit trails can track and trace the following information related to transactions:

Who initiated, approved, modified, or deleted a transaction

When a transaction occurred (date and time)

Where a transaction took place (location or device)

What type of transaction was performed (action or operation)

Why a transaction was executed (purpose or reason)

By analyzing audit trails, an IS auditor can verify whether transactions have been executed by authorized employees or not. Audit trails can also identify any unauthorized, fraudulent, or erroneous transactions that may have occurred. Audit trails can also help to resolve any disputes or discrepancies that may arise from transactions.

References:

What Is an Audit Trail? Everything You Need to Know

NEW QUESTION: 411

IS □□□□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □□□□. □□ □ □□□ □ □□ □ □□□□ □□ □□□□?

A. □□□□□ □□ □ □□

B. □□□□□ □□ □□

C. □□□□□ □□ □□

D. □□□□□ □□ □□□□ □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 412

□□□ □□ □□ □□□ □□□ □□□ □ □□ □□□ □□□ □□□□□?

A. □□ □ □□ □□

B. □□ □□□□ □□

C. □□ □□ □□□□□□□ □□

D. □□ □□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 413
□□ □ IS □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□□ □□ □□□ □□□ □□□□□.
B. □□ □□□□ IT □□□□□ □□□ □□□□□.
C. □□ □□□□ □□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □.
D. □□ □□□□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 414
□□ □ □□ □□ □□□□□ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□□ □ □□ □□□ □ □□□□.
B. □□□ □□ □□□ □ □ □□□□ □□□□□□ □□□□.
C. □□ □□ □□□ □□□□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The most importantoutcome of an information security program is to improve the organizational awareness of security responsibilities, as this will foster a culture of security and ensure that all stakeholders are aware of their roles and obligations in protecting the information assets of the organization. An information security program should also aimto achieve other outcomes, such as identifying operating system weaknesses, understanding and accepting emerging security technologies, and reducing the cost to mitigate information security risk, but these are not as important as improving the awareness of security responsibilities, which is the foundation of any effective information security program. *References: According to the ISACA IT Audit and Assurance Standards, Guidelines and Tools and Techniques for IS Audit and Assurance Professionals, section 2402 Planning, "The IS audit and assurance professional should identify and assess risk relevant to the area under review." 1 One of the risk factors to consider is "the level of awareness of management and staff regarding IT risk management" 1. According to the ISACAIT Audit and Assurance Guideline G13 Information Security Management, "The objective of an information security management audit /assurancereview is to provide management with an independent assessment relating to the effectiveness of information security management within the enterprise." The guideline also states that "the audit/assurance professional should evaluate whether there is an appropriate level of awareness throughout the enterprise regarding information security policies, standards, procedures and guidelines." According to a web search result from Microsoft Security, "Information security programs need to: ... Support the execution of decisions." 2 One of the ways to support the execution of decisions is to ensure that

everyone in the organization understands their security responsibilities and follows the security policies and procedures.

NEW QUESTION: 415
□□ □□□□□ □□ IS □□□□ □□□□ □□ □□□ □□ □□ □□□□ □□□ □ □ □□ □□□□□. □□□□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□□ BEST □□□ □□□ □ □□□□?
A. □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□□ □□ □□□ □□ □□□.
B. □□□ □□ □ □□ □□□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
C. □□□□ □□□ □□ □□(DLP) □□□ □□□□ □□□□□□ □□□□□.
D. □□□□ □□□ □□□ □□ □□ □□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The best way to validate that appropriate security controls are in place to prevent data loss is to review compliance with data loss and applicable mobile device user acceptance policies. This will ensure that the organization has established clear rules and guidelines for employees to follow when connecting their personal devices to company-owned computers. A walk-through, a DLP tool configuration, and a security awareness training are not sufficient to validate the effectiveness of the controls, as they may not cover all possible scenarios and risks. References: IT Audit Fundamentals Certificate Resources

NEW QUESTION: 416
IS □□□□ □□ □□ □□(CSA) □□□□□ □□□ □□□□□ □□□ □□□□□. □□ □ □□□□□□ □□□□ □□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□□ □□□□ □□ □□□ □□□□ □□□.
B. □□□□ □□□□ □□□ □□□ □□□□ □□□.
C. □□□□ □□□□ □□□ □□□ □□ □□□.
D. □□□□ □□□ □□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 417
□□□ □□ □□□ □□□□ □□ IS □□□□ IT □□ □□□ □□□ □□ □□□ □□□ □ □□□ □□ □ □□ □□□ □□ □□□ □□ □□□□□□.
□□□ □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□?
A. □□□□□□ □□□□□ □□□□□.
B. □□ □□□□□ □□□□□.
C. □□ □□□ □□□□□.
D. □□ □□ ID□ □□□□□□.
Answer: A (LEAVE A REPLY)
The best recommendation to help prevent the situation where IT support staff were put in a position to make decisions beyond their level of authority during the review of a system

disruption incident is to introduce escalation protocols. Escalation protocols are policies and procedures that define who should be notified, involved, or consulted when an incident occurs, how the communication and handover should take place, and what criteria or triggers should be used to escalate the incident to a higher level of authority or expertise2. Escalation protocols help to ensure that:
Incidents are handled by the appropriate staff with the required skills, knowledge, and experience Incidents are resolved in a timely and effective manner Incidents are escalated to senior management or specialized teams when necessary Incidents are documented and reported accurately and transparently Incidents are analyzed and learned from to prevent recurrence or mitigate impact Therefore, by introducing escalation protocols, an organization can improve its incident management process and avoid putting IT support staff in a position to make decisions beyond their level of authority.
References:
Escalation policies for effective incident management, Section 1: What is incident escalation?

NEW QUESTION: 418
□□ □ □□ □□□□ □□ □□□□□ □□□□ □□ □□ □□□□□□ □□□ □□□ □□□ □□□□ □□ □□□□?
A. □□□ □□ □□□(UAT)
B. □□□□ □□□
C. □□□□ □□□
D. □□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 419
□□□ □□□□ □□ □□□□ □□□ □□□□ IS □□□□□ □□ □□□ □□□ □□□ □□?
A. □□□ □□ □□□ □□□ □□□□.
B. □□□ □□□□ □ □□□ □□ □□□ □□□□ □□□□□.
C. □□ □□□ □□ □□□□□ □□□□ □□□□.
D. □□□□ □□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
he design of an incident management process should include prioritization criteria to ensure that incidents are handled according to their impact and urgency. Without prioritization criteria, the organization may not be able to allocate resources effectively and respond to incidents in a timely manner. Expected time to resolve incidents, service management standards, and metrics reporting are important aspects of incident management, but they are not as critical as prioritization criteria for the design of the process. References: ISACA Journal Article: Incident Management: A Practical Approach

NEW QUESTION: 420
□ □□□□ □□ □□□□ □□ □□ □□ □□ □□□ □ □□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□. □□ □ □ □□□ □□□ □□ □ □□□ □□□□□?
A. □□ □□ □□
B. □□□ □□ □□
C. □□□ □□ □□□□□□ □□ □□□
D. IT □□ □□ □□
Answer: C (LEAVE A REPLY)
Real-time replication to a second data center means that any changes made to the primary data center are immediately copied to the secondary data center. This can improve data availability and performance, but also introduces the risk of propagating malicious or erroneous changes to the backup data center. If a cybersecurity attack compromises the primary data center, it may also affect the secondary data center, making it difficult or impossible to recover from the attack using the replicated data. Therefore, option C is the greatest risk associated with this change.
Option A is not correct because version control issues are more likely to occur with batch processing backup, which may create inconsistencies between different versions of the data. Option B is not correct because real- time replication may reduce system performance at the primary data center, but it may also improve system performance at the secondary data center by reducing latency and network traffic. Option D is not correct because although real-time replication may increase IT investment cost, this is not a risk but a trade-off that the organization has to consider.
References:
Data Replication: The Basics, Risks, and Best Practices1
Best Practices for Data Replication Between Data Centers2
The Good, Bad, and Ugly of Data Replication3

NEW QUESTION: 421
□□ □ □□□ □□□ □□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. USB □□ □□□□
B. □□ □□□ □□□
C. □□ □□ □□ □□
D. 2□□ □□
Answer: B (LEAVE A REPLY)
The best method to safeguard data on an organization's laptop computers is full disk encryption. Full disk encryption is a technique that encrypts all the data stored on a hard drive, including the operating system, applications, files, and folders. This means that if the laptop is lost, stolen, or accessed by an unauthorized person, they will not be able to read or modify any data without knowing the encryption key or password. Full disk encryption provides a strong level of protection for data at rest, as it prevents data leakage or exposure in case of physical theft or loss of the device.

References:
* How to Protect the Data on Your Laptop
* 6 Steps to Practice Strong Laptop Security

NEW QUESTION: 422
□□ □□□□ □□□□□□□ 1□□ □□□□□□ □□□ □□□□□. □□ □□□ □□ □□□□□□ □□□□ □□□□ □□□ □□□□ □□ □□□□ □□□□□□ □□□ □ □□□□□. □□ □ IS □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□□ □□□ □□
B. □□□□□□ □□□□ □□ □□ □□
C. □□□ □□□□□□ □□ □□□ □□□□.
D. □□ □□ □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 423
□□ □ □□□□□ □□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□ □ □ □□□ □□□□□?
A. □□
B. □□□ □□
C. □□□
D. □□□
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Normalizationis the process ofstructuring log datainto a standard format for easy analysis and correlation across multiple systems.
* Normalization (Correct Answer - D)
* Ensures consistency in log file formats.
* Helps security analysts detect patterns and anomalies.
* Example:Converting log timestamps into a standardized format (UTC).
* Extraction (Incorrect - A)
* Retrieves data but does not format it for analysis.
* Data Acquisition (Incorrect - B)
* Refers to collecting data, not structuring it.

* Imaging (Incorrect - C)
* Creates copies of disk storage but is unrelated to log analysis.
References:
* ISACA CISA Review Manual
* NIST 800-92 (Guide to Computer Security Log Management)

NEW QUESTION: 424
□□ □ IS □□□□ □□□ □□□□□□□ □□□ □□□ □□ □□□ □□□□ □□□ □ □□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□(ITF)
B. □□□
C. □□□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
Data analytics is the process of analyzing large and complex data sets to discover patterns, trends, and insights that can support decision making and problem solving. Data analytics can enable an IS auditor to combine and compare access control lists from various applications and devices by using techniques such as data extraction, transformation, loading, cleansing, integration, aggregation, visualization, and reporting. Data analytics can help an IS auditor to identify and assess the risks and controls related to access management, such as unauthorized or excessive access, segregation of duties violations, access policy compliance, access activity monitoring, and access review and remediation.
The other options are not as effective or relevant as data analytics for combining and comparing access control lists from various applications and devices. Integrated test facility (ITF) is a technique for testing the validity and accuracy of application processing by inserting fictitious transactions into the system and verifying the results. ITF does not directly involve the analysis of access control lists. Snapshots are records of selected information at a specific point in time that can be used to monitor system activity or performance.
Snapshots can provide some information about access control lists, but they are not sufficient to combine and compare them across different sources. Audit hooks are software routines embedded in an application that can trigger an alert or a report when certain conditions are met. Audit hooks can help to detect anomalies or exceptions in access control lists, but they do not provide a comprehensive or integrated view of them.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 2361
ISACA, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, 2014, p. 882 Data Analytics for Auditing Access Control3

NEW QUESTION: 425

IS □□ □□□ IT □ □□□□ □□□□ □□□ □□ □□□ □□□□□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□. □□□ □□□ □□□□□ □□□□ □□ □□□ □□□□□□□. □□ □ □□ □ □□ □□□ □□□□□?

A. □□□ □□□ □□□ □□

B. □□□ □□□ □□□ □□□

C. □□□ □□□ □□□ □□

D. □□□ □□□ □□□□ □□□□□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 426

□□ □□□□ □□□ □ □□ □□□□ □□ □□ □□□ □□□□□□ □□□ □□□□ □. □ □□□ □□□ □□□ □□□□ □ □□□ □□ □□□ □□□ □ □□□ □□□□□. □□□ □□□ □□ □□ □□ □ □□ □ □□□ □□ □□□ □□□□□?

A. □□□

B. □□ □

C. □□

D. □□

Answer: C (LEAVE A REPLY)

The risk that is most affected by this oversight is audit risk. Audit risk is the risk that the auditor may express an inappropriate opinion or conclusion based on the audit evidence obtained. Audit risk consists of inherent risk, control risk, and detection risk. Inherent risk is the risk that material errors or frauds exist in the audited area before considering the effectiveness of internal controls. Control risk is the risk that the internal controls fail to prevent or detect material errors or frauds. Detection risk is the risk that the auditor fails to identify material errors or frauds using the audit procedures performed. In this case, the auditor has overlooked evidence that could contradict a conclusion of the audit, which increases the detection risk and consequently the audit risk. References:

* CISA Review Manual (DigitalVersion), Chapter 2, Section 2.31
* CISA Online Review Course, Domain 1, Module 1, Lesson 32

NEW QUESTION: 427

IT□ □□□□ □□□ □□ □□□□□□ □□□ □ IS □□□□ □□ □□□□ □□□□ □ □□□ □□□ □□□□.

A. □□□ □□ □□□ □□ □□ □□□ □□□□□.

B. IT □□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□□□.

C. □□□ IT □□□□□ □□□□□□ □□ IT □□□□□□ □□□□□.

D. □□□ □□□□ □□□□ □□ □□□ IT □□□□□□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

When auditing the alignment of IT to the business strategy, it is most important for the IS auditor to evaluate deliverables of new IT initiatives against planned business services. This can help the IS auditor to assess whether the IT initiatives are meeting the business

needs and expectations, delivering value and benefits, and supporting the business objectives and goals. Comparing the organization's strategic plan against industry best practice is a possible technique for auditing the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as industry best practice may not be applicable or relevant to the specific context or situation of the organization. Interviewing senior managers for their opinion of the IT function is a possible technique for auditing the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as senior managers' opinions may be subjective or biased, and may not reflect the actual performance or outcomes of the IT function. Ensuring an IT steering committee is appointed to monitor new IT projects is a possible control for ensuring the alignment of IT to the business strategy, but it is not the most important thing for the IS auditor to do, as an IT steering committee may not be effective or efficient in monitoring new IT projects, and may not have sufficient authority or influence over the IT function.

NEW QUESTION: 428
IS □□□□ □□□ □□□ □□ □□(DLP) □□□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□ □□□ □□□□□□. □□□□ □□ □□□□ □□□ □□□ □.
A. □□□ □□ □□□□ □□ □□ □□□□ □□□□ □□ □□ □□□□.
B. □□ □□□ □□□ □□□□ □□ □ □□□□.
C. □□ □□□ □□□ □□ □□□□ □□ □□□ □ □□□□.
D. □□□□ □□ □□ □□□ □□□ □ □□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 429
□□□□□□ ERP(□□ □□ □□) □□□□ □□□□ □□, □□□ □□□ □□□ □□ □ □ □□□ □□ □□□ □□□□□?
A. □□ □□
B. □□□ □□□
C. □□ □ □□ □□
D. □□□□ □□
Answer: D (LEAVE A REPLY)
The most important consideration for a go-live decision when implementing an upgraded enterprise resource planning (ERP) system is the business case. The business case is the document that defines and justifies the need, value, feasibility, and risks of the project. It also outlines the expected costs, benefits, outcomes, and impacts of the project. The business case provides the basis for measuring and evaluating the success of the project. Therefore, before deciding to go live with an upgraded ERP system, it is essential to review and validate the business case to ensure that it is still relevant, accurate, realistic, and achievable.

A rollback strategy, test cases, and post-implementation review objectives are not the most important considerations for a go-live decision when implementing an upgraded ERP system. These are important elements of project planning, execution, and evaluation, but they are not sufficient to determine whether the project is worth pursuing or delivering. These elements should be aligned with and derived from the business case.

NEW QUESTION: 430
□□ □ □□ □□□□ □□□□ □□□□□ □□ □□□ □□ □□□ □□□□ □□□ □ □□ □□ IT □□ □□ □□□ □□□□ □□ □□□ □□ □□□?
A. □□ □□□□ □□□ □□□ □□□□ □□ □□ □□□□ □□□□□.
B. □□ □□□□ □□ □□□□ □□□ □□□ □□□□□ □□□.
C. □□ □□□□ □□ □□ □□□ □□□□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
The best approach to optimize resources when both internal and external audit teams are reviewing the same IT general controls area is to leverage the work performed by external audit for the internal audit testing. This can avoid duplication of efforts, reduce audit costs and enhance coordination between the audit teams. The internal audit team should evaluate the quality and reliability of the external audit work before relying on it.
Ensuring both the internal and external auditors perform the work simultaneously is not an efficient use of resources, as it would create redundancy and possible interference. Requesting that the external audit team leverage the internal audit work may not be feasible or acceptable, as the external audit team may have different objectives, standards and independence requirements. Rolling forward the general controls audit to the subsequent audit year is not a good practice, as it would delay the identification and remediation of any control weaknesses in a high-risk area. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
247

NEW QUESTION: 431
□□ □ □□□□□□ □□□□□ □□□□□(API) □□ □□□ □□□ □□ □□□ □□□ □ □□ IS □□□□ □□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□(XML) □□□ □□□□□□.
B. □□ □□ □□(TLS)□ □□□□□.
C. SOAP(Simple Object Access Protocol)□ □□□□□.
D. API □□□□□□ □□□□□□.
Answer: (SHOW ANSWER)
The best recommendation to mitigate the risk of eavesdropping associated with an API integration implementation is to implement Transport Layer Security (TLS). TLS is a cryptographic protocol that provides secure communication over a network by encrypting the data in transit and authenticating the parties involved. TLS can prevent unauthorized

parties from intercepting, modifying or tampering with the data exchanged between the API endpoints. Encrypting the XML file, implementing SOAP, and masking the API endpoints are not sufficient to mitigate the risk of eavesdropping, as they do not provide end-to-end encryption or authentication for the API communication. References: IS Audit and Assurance Tools and Techniques, CISA Certification | Certified Information Systems Auditor | ISACA

NEW QUESTION: 432
□□ □□□□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□□□□ □□ □□ □ □□□.
A. □□ □□ □□□□ □□ □□□ □□□□□□ □□ □□□ □□□□□.
B. □□ □□□ □□□□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□□.
C. □ □□□□□ □□□□ □□ □□□ □□□□□□.
D. □□□□□□ □□□ □□ □□□ □□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
Controls related to authorized modifications to production programs are best tested by tracing modifications from the original request for change forward to the executable program, as this ensures that the change management process was followed and that the modifications were approved, documented, tested, and implemented correctly. Tracing modifications from the executable program back to the original request for change may not reveal any unauthorized or undocumented changes that occurred during the process. Testing only the authorizations to implement the new program or reviewing only the actual lines of source code changed in the program are not sufficient to test the controls related to authorized modifications, as they do not cover the entire change management process. References: CISA Review Manual (Digital Version), Chapter 4: Information Systems Operations, Maintenance and Service Management, Section 4.2: Change Management

NEW QUESTION: 433
□□ □ □□ □□□ □□□□ □□□ □□□ □□□ □□□□ □□ □ □□□□ □□ □□ □□□?
A. □□□□ □□□ □□ □□ □□ □□ □ □□
B. □□ □□□ □□□ □□ □ □□
C. □□ □□□ □ □□□ □□ □□ □□
D. □□ □□□ □ □□ □□ □□
Answer: D (LEAVE A REPLY)
The best way to ensure the quality and integrity of test procedures used in audit analytics is to centralize procedures and implement change control. Centralizing procedures means storing themin a common repository that can be accessed and updated by authorized users. Change control means implementing a process for tracking, reviewing, approving, and documenting any changes made to the procedures. This ensures that the procedures are consistent, accurate, reliable, and secure. References: CISA Review Manual,

NEW QUESTION: 434
□□ □ □□□□□□ □□□□(EA) □□□ □□□□□ □□ □□ □□ □□□ □□□□ □?
A. IT □□ □ □□ □□□□ □□ □□□ □□
B. □□□ □□□ □□
C. □□ □□□□ □□ □□□□ □□□ □□□□ □□□
D. □□□ □ □□□ □□□□ □□□□
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:Enterprise Architecture (EA) documentation primarily includes strategic and operational blueprints outlining the evolution of IT infrastructure to align with business goals. Roadmaps showing the evolution from current state to future state (C) are essential for understanding how the organization's IT environment will change over time to support business strategy.
Other options:
* Contact information for key resources (A) is more of an operational or administrative document rather than an EA component.
* Detailed encryption standards (B) would typically be found in security policies or system-specific documentation rather than in EA documentation.
* Protocols used to communicate between systems (D) are typically documented within network or system architecture diagrams rather than high-level EA documentation.
Reference: ISACA CISA Review Manual, IT Governance and Management of IT

NEW QUESTION: 435
□□□□□□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□. □□ □ □□ □ □ □□□ □ □□□ □□ □ □□□ □□□□□?
A. □□□□□□ □□□□ □□□□ □□□□□ □□□□□.
B. □□□ □□ □□□ □□□□□ □□□□□.
C. □□□□□□ □□□□ □□□□□ □□□□ □ □□□□.
D. □□ □□□ □□□ □□□ □□ □□□□□.
Answer: C (LEAVE A REPLY)
The programmer having access to the production programs is a control weakness that would have contributed most to the problem of unauthorized changes to key fields in a payroll system report. This is because it violates the principle of segregation of duties, which requires that different individuals or groups perform different functions related to system development, testing, implementation, and operation. Allowing programmers to access production programs increases the risk of errors, fraud, or malicious actions that may compromise the integrity, availability, or confidentiality of the system or its data. The other options are not as significant as having access to production programs, as they relate to other aspects of system development or maintenance, such as user involvement

in testing (which affects user satisfaction and acceptance), user requirements documentation (which affects system functionality and quality), and payroll files control (which affects data security and accuracy). References: CISA Review Manual (Digital Version), Domain 3:
Information Systems Acquisition, Development and Implementation, Section 3.2 Project Management Practices

NEW QUESTION: 436
□□□□ □□ □□□□ □□□ □ □□ □ □□ □□□□□ □□□□ □□□?
A. □□□ □□□□□ □□□□(UDP)
B. □□□□□□ □□ □□□□(HTTP)
C. □□ □□ □□ □□□□(SFTP)
D. □□ □□□□ □□□□(RDP)
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
SFTP (Secure File Transfer Protocol)is the most secure option for transferring data over the internet, as it encrypts both commands and data, ensuring confidentiality and integrity.
* SFTP (Correct Answer - C)
* Uses SSH (Secure Shell) for encryption.
* Provides authentication and encryption for secure data transfers.
* Example:A company uses SFTP to securely transmit payroll files to a third-party processor.
* UDP (Incorrect - A)
* Faster but lacks encryption and data integrity checks.
* HTTP (Incorrect - B)
* Transfers data in plaintext and is vulnerable to interception.
* RDP (Incorrect - D)
* Used for remote desktop access, not secure file transfers.
References:
* ISACA CISA Review Manual
* NIST 800-52 (Guidelines for Transport Layer Security)

NEW QUESTION: 437

□□ □□□ □□□ □□□ □□ □□□ □□□□ IS □□□□□ □ □□□ □□□ □□□ □□□□□□. □□ □ □□□□□ □□ □ □□□□ □□□□□?
A. □□ □□□ □□□□ □□ □□ □□□ □□□□□ □□□ □□□□□.
B. □□ □□□ □□□□ □□□ □□□ □□□□□.
C. □□ □□ □□□□ □□□ □□□ □□□□ □□ □□□□□.
D. □□ □□□ 12□□ □□ □□ □□ □□□□□ □□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 438
IT □□□□□ □□□ □□□ □□, □□□ □□ □□□□□ □□□□ □□ □□□ □□□□ □□□□ □□□□□ □□ □□□ □□□□□□. □□ □ IS □□□□ □□ □□□□ □□ □□□□□?
A. □□□ □□□ □□ □□□, □□□ □ □□ □□□ □□□□□□.
B. □□□ □ □□□ □□ □□□ □□□□ □□□□□ □□
C. □□□ □□□ □ □□□□ □□□□ □□□□□ □□□.
D. □□□ □ □□□ □ □□□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)
The best recommendation for an organization that does not have a process to identify and correct records that do not get transferred to the receiving system is to implement software to perform automatic reconciliations of data between systems. This will ensure that the data integrity and completeness are maintained and that any errors or discrepancies are detected and resolved in a timely manner. Enabling encryption, decryption, and electronic signing of data files may enhance the data security and authenticity, but not the data accuracy or consistency. Having coders perform manual reconciliation of data between systems may be prone to human errors and inefficiencies. Automating the transfer of data between systems as much as feasible may reduce the chances of data loss or corruption, but not eliminate them completely. References: IS Audit and Assurance Standards, section "Standard 1202: Risk Assessment in Planning"

NEW QUESTION: 439
□□ IT □□□□□ □□□ □ IS □□□ □□□□□ □□ □□□ □□□ □□□□□?
A. □□□□□□ IT □□□□ □□□□□□ □□ □□ □□ □□
B. □□ □□□ □□ □□ □□ □ □□□□□ □□ □□ □□
C. □□, □□ □ □□ □□ □□□ □□□□□ □□
D. IT □□□□ □□□ □□□□ □□ □□□□□ □□□□ □□□ □□
Answer: D (LEAVE A REPLY)
The most important benefit of involving IS audit when implementing governance of enterprise IT is providing independent and objective feedback to facilitate improvement of IT processes.Governance of enterprise IT is the process of ensuring that IT supports the organization's strategy, goals, and objectives in an effective, efficient, ethical, and compliant manner. IS audit can provide value to governance of enterprise IT by assessing

the alignment of IT with business needs, evaluating the performance and value delivery of IT, identifying risks and issues related to IT, recommending corrective actions and best practices, and monitoring the implementation and effectiveness of IT governance activities. IS audit can also provide assurance that IT governance processes are designed and operating in accordance with relevant standards, frameworks, laws, regulations, and contractual obligations. Identifying relevant roles for an enterprise IT governance framework is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help define and clarify the roles and responsibilities of various stakeholders involved in IT governance, such as board members, senior management, business units, IT function, external parties, etc. IS audit can also help ensure that these roles are aligned with the organization's strategy, goals, and objectives, and that they have adequate authority, accountability, communication, and reporting mechanisms. However, this benefit is more related to the design phase of IT governance implementation than to the ongoing monitoring and improvement phase. Making decisions regarding risk response and monitoring of residual risk is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help identify and assess the risks associated with IT activities and processes, such as strategic risks, operational risks, compliance risks, security risks, etc. IS audit can also help evaluate the effectiveness of risk management practices and controls implemented by management to mitigate or reduce these risks. However, this benefit is more related to the assurance function of IS audit than to its advisory function. Verifying that legal, regulatory, and contractual requirements are being met is a benefit of involving IS audit when implementing governance of enterprise IT, but not the most important one. IS audit can help verify that IT activities and processes comply with applicable laws, regulations, and contractual obligations, such as data protection laws, privacy laws, cybersecurity laws, industry standards, service level agreements, etc. IS audit can also help identify and report any instances of noncompliance or violations that could result in legal or reputational consequences for the organization. However, this benefit is more related to the assurance function of IS audit than to its advisory function. References: ISACA CISA Review Manual 27th Edition, page 283

NEW QUESTION: 440

□□□□ □□ □□□ □□ □□□ □□□ □ IS □□□□ □□ □□□ □□□□ □□□ □ □□□ □□□□ □□□□ □□□ □ □□□ □□□□□. □□ □ □□□□ □□□ □□ □ □□ □□□□□?

A. □□ □□□□□ □□□□.

B. □□ □□□ □□□□□□.

C. □□ □□□□□ □□□□.

D. □□□□ □□□□ □□ □□ □□□ □□ □□□□□.

Answer: C (LEAVE A REPLY)

If an IS auditor suspects that independence may not have been maintained in past audits, the best course of action is to inform audit management. Audit management has the responsibility and authority to address such issues. They can review the situation, determine if there was indeed a lack of independence, and decide on the appropriate actions to take123. While informing senior management, reevaluating internal controls, and re- performing past audits might be necessary at some point, the first step should be to inform audit management.

NEW QUESTION: 441
□□□ □□□□□ □□ □□□□□□ □□□ □□ □□ □□□ □□□□ □□ □□□ □□ □□□□. □□ □□□ □□□ □□□ □□ □□ □ □□□□. □□□□□ □□□ □□□□ □□□□□ □□□□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□□□. □□ □□ □□ □ □□ □□ □□ □□ □□□□ □□□ □□ □□ □□□□□?
A. □□□ □□ □□□ □□ □□□ □□□□□.
B. □□□ □□□ □□ □□ □□ □□□ □□□□□.
C. □□□ □ □□ □3□□□ □□□ □□ □□□ □□□□□□□.
D. □□ □□□ □□□ □□□□ □□□□ □□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
Implementing business rules to validate employee data entry is the best way to reduce the likelihood of future occurrences of poor data quality that cause customer complaints about receiving different items from what they ordered on the organization's website. Business rules are logical statements that define the conditions and actions for data validation, such as checking for data completeness, accuracy, consistency, and integrity. Assigning responsibility for improving data quality, investing in additional employee training for data entry, and outsourcing data cleansing activities to reliable third parties are also possible ways to improve data quality, but they are not as effective as implementing business rules to validate employee data entry. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.3.1

NEW QUESTION: 442
□□ □□□ □□□□ □ □□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□ □ □□□□?
A. □□□ □□ □□□(UAT)
B. □□□ □□□
C. □□ □□□
D. □□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 443
□□ □ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□□.

B. □□□ □□□ □□□ □□□ □□□□□.
C. □□□ □□ □□□□□ □□□.
D. □□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 444
□□□ □□□ □□□ IT □□□ □□□□□ □□□□ □□ □□□ □ IS □□□□ □□□ □□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□ □□□(ROIs)□ □□ □□□ □□□□ □□
B. □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□□.
C. □□□□ □□□□ □□ □□□ □□□□□.
D. □□□ □□ □□ □□(KPIs)□ □□□□□.
Answer: C (LEAVE A REPLY)
The best approach for an IS auditor to evaluate whether the IT strategy supports the organization's vision and mission is to meet with senior management to understand the business goals and how IT can enable them.
This will help the IS auditor to assess the alignment and integration of IT with the business strategy and to identify any gaps or opportunities for improvement. Reviewing ROIs, KPIs, or feedback from other departments may provide some insights, but they are not sufficient to evaluate the IT strategy. References: IS Audit and Assurance Standards, section "Standard 1201: Engagement Planning"

NEW QUESTION: 445
IS □□□□ □□□ □□□□ □□□ □□ □□□□ □□ ERP(Enterprise Resource Planning) □□□ □□ □□□ □□□□□ □□ □□□□□□. □ □□ □□□ □□□□□ □□□ □ □□□□ □ □□ □□□□ □□□ □□ □ □□ □□□□?
A. ERP □□□□ □□□ □□ □□
B. □□ □□□ □□□ □□ □□
C. □□ □□□ □□
D. □□□□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 446
□□ □ □□□ □□□ □□□□ □□ □ □□□□ □□ □□□□□?
A. RAID □□ 5 □□ □□
B. □□□ □□
C. □□ □□□ □□ □□□□ □□□
D. □□□□□ □□□□
Answer: C (LEAVE A REPLY)
The primary benefit of automating application testing is to provide test consistency. Automated testing can ensure that the same test cases are executed in the same manner

and order every time, which can improve the reliability and accuracy of the test results. Providing more flexibility, replacing all manual test processes, and reducing the time to review code are possible benefits of automating application testing, but they are not the primary benefit. References:
* ISACA, CISA Review Manual, 27th Edition, 2020, p. 3091
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 447
□□□□□ RFID□ □□□ □ IS □□□□ □□ □□□□ □ □□ □□□□□?
A. □□□□□□
B. □□□□□
C. □□ □□
D. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 448
□□ □□ □ IS □□□□□ □□ □□ □□□ □ □□ □□□□ □□ □□ □□□□ □□ □ □ □□ □□□□ □□□□ □□ □□□□□?
A. □□ □□ □□
B. □□□ □□ □□ □□
C. □□ IT □□□ □□□
D. IT □□□□□ □□□ □□
Answer: (SHOW ANSWER)
Mapping IT processes to roles is an activity that provides an IS auditor with the most insight regarding potential single person dependencies that might exist within the organization. Single person dependencies occur when only one person has the knowledge, skills, or access rights to perform a critical IT function.
Mapping IT processes to roles can help to identify such dependencies and assess their impact on the continuity and security of IT operations. The other activities do not provide as much insight into single person dependencies, as they do not show the relationship between IT processes and roles. References: CISA Review Manual, 27th Edition, page 94

NEW QUESTION: 449
□□ □□□□ □□□ □ □□ □□ □□ □ □□ □□□□□?
A. □□ □□ □□(NDA)□ □□□□□.
B. □□□ □□ □□ □□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□ □□□□.
Answer: D (LEAVE A REPLY)

The first step when planning a penetration test is to obtain management consent for the testing. This is because a penetration test involves simulating a cyberattack against the organization's systems and networks, which may have legal, ethical, and operational implications. Without proper authorization from management, a penetration test may violate laws, policies, contracts, or service level agreements. Management consent also helps define the objectives, scope, and boundaries of the test, as well as the roles and responsibilities of the testers and the stakeholders. Obtaining management consent for the testing also demonstrates due care and due diligence on the part of the testers and the organization.
Executing nondisclosure agreements (NDAs), determining reporting requirements for vulnerabilities, and defining the testing scope are important steps when planning a penetration test, but they are not the first step.
These steps should be done after obtaining management consent for the testing, as they depend on the approval and involvement of management and other parties.

NEW QUESTION: 450
□□ □ □□ □□□ □□□ □ □□□ □□□□ □□□□□□ □□□□ □ □□ □□□ □ □□ □□□ □□□□□?
A. □□ □□□
B. □□ □□□
C. □□ □□□
D. □□ □□□
Answer: A (LEAVE A REPLY)
Regression testing is the most appropriate testing method for assessing whether system integrity has been maintained after changes have been made. Regression testing is a type of software testing that ensures that previously developed and tested software still performs as expected after a change1 Regression testing helps to detect any defects or errors that may have been introduced or uncovered due to the change2 Regression testing can be performed at different levels of testing, such as unit, integration, system, and acceptance3 Unit testing is a type of software testing that verifies the functionality of individual components or units of code. Unit testing is usually performed by developers before integrating the code with other components. Unit testing helps to identify and fix errors at an early stage of development, but it does not ensure that the system as a whole works as expected after a change.
Integration testing is a type of software testing that verifies the functionality, performance, and reliability of the interactions between different components or units of code. Integration testing is usually performed after unit testing and before system testing. Integration testing helps to identify and fix errors that may occur when different components are integrated, but it does not ensure that the system as a whole works as expected after a change.
Acceptance testing is a type of software testing that verifies whether the system meets the user requirements and expectations. Acceptance testing is usually performed by end-users

or customers after system testing and before deploying the system to production. Acceptance testing helps to ensure that the system delivers the desired value and quality to the users, but it does not ensure that the system as a whole works as expected after a change.
References: 1: What is Regression Testing? Test Cases (Example) - Guru99 2: What is Regression Testing? Definition, Tools, Examples - Katalon 3: Regression testing - Wikipedia : What is Unit Testing?
Definition, Types, Tools & Examples - Guru99 : What is Integration Testing? Definition, Types, Tools & Examples - Guru99 : What is Acceptance Testing? Definition, Types, Tools & Examples - Guru99

NEW QUESTION: 451
□□ □ □□□ □□□ □□ □□ □□□ □□□ □□□□ □□ □ □□ □□ □□□ □□□ □□?
A. □□ □□
B. □□ □□
C. □ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
Water sensors are devices that can detect the presence of water or moisture in a given area. They are often deployed below the floor tiles of a data center to monitor for any water leaks that may damage the equipment or cause electrical hazards. Water sensors can alert the data center staff or trigger an automatic response to prevent or mitigate the water leakage.
The other options are not likely to be deployed below the floor tiles of a data center. Temperature sensors and humidity sensors are usually deployed above the floor tiles to measure the ambient conditions of the data center and ensure optimal cooling and ventilation. Air pressure sensors are typically deployed at the air vents or ducts to monitor the airflow and pressure distribution in the data center.
References:
* Data Center Environmental Monitoring
* Water Detection in Data Centers

NEW QUESTION: 452
□□ □ □□□ □□□ □□□ □□□□ □□□ □ □□□ □□ IS □□□□ □□ □□ □□ □□□ □□□□□?
A. □□□ □□
B. □□□
C. □□□□□□(CPU) □□□□
D. □□□□ □□□□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 453
IS □□□□ □□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□.
□□ □ □□ □□□□□ □□□□ □□□ □□□□□?
A. □□□ □□□□ □□ □□ □□□□ □□□□ □□□□□.
B. □□□ □□ □□ □□□(IDS)□ □□ □□□□ □□□□ □□□□□.
C. □□□ □□□ □□□ □□□ □ □□□□.
D. □□□ □□ □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
The most critical finding for an IS auditor following up on a recent security incident is that the security weakness facilitating the attack was not identified. This finding indicates that the root cause of the incident was not analyzed, and the vulnerability that allowed the attack to succeed was not remediated. This means that the organization is still exposed to the same or similar attacks in the future, and its security posture has not improved. Identifying and addressing the security weakness is a key step in the incident response process, as it helps to prevent recurrence, mitigate impact, and improve resilience.
The other findings are not as critical as the failure to identify the security weakness, but they are still important issues that should be addressed by the organization. The attack was not automatically blocked by the intrusion detection system (IDS) is a finding that suggests that the IDS was not configured properly, or that it did not have the latest signatures or rules to detect and prevent the attack. The attack could not be traced back to the originating person is a finding that implies that the organization did not have sufficient logging, monitoring, or forensic capabilities to identify and attribute the attacker. Appropriate response documentation was not maintained is a finding that indicates that the organization did not follow a consistent and formal incident response procedure, or that it did not document its actions, decisions, and lessons learned from the incident.
References:
* ISACA CISA Review Manual 27th Edition (2019), page 254
* Incident Response Process - ISACA1
* Incident Response: How to Identify and Fix Security Weaknesses

NEW QUESTION: 454

□□ □ □□ □□□ □□□(EUC) □□□□□□□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□?

A. □□ □□□ □□□ □ □□□ □□

B. □□ □□□ □□□ □□□□□□□ □□□□□ □□□□□.

C. □□□ □□□ □□□□□□□ □□□□ □□□□ □□

D. □□□ □□□□ □□□□□□□ □□□□ □ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

Version control is a process of managing changes to an application or a document. It ensures that only the latest approved version of the application is used by end-users, which reduces the risk of errors, inconsistencies, and unauthorized modifications. Version control also allows tracking the history of changes and restoring previous versions if needed.

NEW QUESTION: 455

IS □□□□ 2□□□ □□ □□□□□□ □□□□ □□□ □□□□ □□□ □□ □ □□ □ □□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□. □□ □ □□□ □□ □ □□□ □□□□ □□ □□□ □□□□□?

A. □□□ □□ □□□ □□

B. □□□ □□ □□□ □□□□□.

C. □□□ □□□ □□ □□□ □□

D. □□□□□ □□□ □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 456

IS □□□□ □□ □□□□ □□□ □□□□ □□□□ □□ □□□ □□□ □□ □□□ □ □□□ □□□□. □□ □ □□□□ □□ □□□□ □ □□ □□□ □□□□□?

A. □□□□□ □ □□□ □□□□ □□□ □□ □□□ □□□□ □□□□□.

B. □□□ □□□□ □□ □□ □ □□□□□ □□□□□ □□ □□□□.

C. □□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□□ □ □□□□.

D. □□ □□□ □□□□□ □□□ □□□□□ □□□□ □□□□ □ □□□□.

Answer: B (LEAVE A REPLY)

The observation that should be of most concern to the auditor when reviewing security controls related to collaboration tools for a business unit responsible for intellectual property and patents is that employees can share files with users outside the company through collaboration tools. Collaboration tools are software or hardware devices that enable users to communicate, cooperate, and coordinate with each other on a common task or project. Collaboration tools can facilitate information sharing and knowledge exchange among users, but they can also pose security risks if not properly controlled or managed. Employees can share files with users outside the company through collaboration tools, as this can compromise the security and confidentiality of intellectual property and patents, which are valuable and sensitive assets of the organization.

Employees may share files with unauthorized or untrusted users who may misuse or disclose the intellectual property and patents, either intentionally or unintentionally. This can cause harm or damage to the organization, such as loss of competitive advantage, reputation, revenue, or legal rights. Training was not provided to the department that handles intellectual property and patents is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Training is an activity that educates and instructs users on how to use collaboration tools effectively and securely, such as how to access, share, store, and protect information using collaboration tools. Training was not provided to the department that handles intellectual property and patents, as this can affect the awareness and competence of users on collaboration tools, and increase the likelihood of errors or mistakes that may compromise the security or quality of information. However, this observation may not be directly related to collaboration tools, as it may apply to any information system or resource used by the department. Logging and monitoring for content filtering is not enabled is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. Logging and monitoring are processes that record and analyze the events or activities that occur on an information system or network, such as user actions, system operations, data changes, errors, alerts, etc. Content filtering is a technique that blocks or allows access to certain types of information based on predefined criteria or rules, such as keywords, categories, sources, etc. Logging and monitoring for content filtering is not enabled, as this can affect the auditability, accountability, and visibility of collaboration tools, and prevent detection or investigation of security incidents or violations related to information sharing using collaboration tools. However, this observation may not be specific to collaboration tools, as it may affect any information system or network that uses content filtering. The collaboration tool is hosted and can only be accessed via an Internet browser is a possible observation that could indicate a security issue related to collaboration tools for a business unit responsible for intellectual property and patents, but it is not the most concerning one. A hosted collaboration tool is a type of cloud-based service that provides collaboration functionality over the Internet without requiring installation or maintenance on local devices. An Internet browser is a software application that enables users to access and interact with web-based content or services. The collaboration tool is hosted and can only be accessed via an Internet browser, as this can affect the availability and reliability of collaboration tools, and introduce security or privacy risks for information sharing using collaboration tools. However, this observation may not be unique to collaboration tools, as it may apply to any cloud-based service that uses an Internet browser.

NEW QUESTION: 457

IS □□□□ □□□ □□ □□□□□ □□□□ □□□□. □□□□ □□□□ □□ □□□□ □□ □□ □□ □□ □□□ □□ □ □□ □□□□?

A. □□□ □□□ □□□□□ □□□□□.
B. □□ □□ □□□□ □□□□□.
C. □□□ □□□□□ □□□□□□.
D. □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 458
□□ □□□ □□□□, □□□ □□□□ □□ □□ □□□ □□□ □□□□□□ □□□?
A. □□ □□
B. □□□ □□
C. □□ □□
D. □□□ □□
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Service accountsare used by applications or systems to perform automated tasks and shouldnot be allowed for interactive login, as they present security risks if compromised.
* Service Accounts (Correct Answer - D)
* Used for running background tasks (e.g., database services, scheduled jobs).
* Should have minimal permissions and be denied interactive logins.
* Example:A compromised service account with interactive login could allow attackers to gain system access.
* Local Accounts (Incorrect - A)
* Local administrator accounts should be restricted but may still be required for some systems.
* Administrator Accounts (Incorrect - B)
* Should be restricted, but disabling them entirely could lock out system management.
* Console Accounts (Incorrect - C)
* Console access is sometimes needed for system recovery and troubleshooting.
References:
* ISACA CISA Review Manual
* NIST 800-63B (Digital Identity Guidelines)
* CIS (Center for Internet Security) Best Practices

NEW QUESTION: 459
□□□ □□□□ □□□ □□□□□ □□ □□□□ □□□ □□□ □ IS □□□□ □□ □ □□□ □□□ □□ □ □□□□□?
A. □□□□ □□ □□ □□□□□ □□□□ □□ □□□□.
B. □□ □□□ □□ □□□ □□□□.
C. □□□□□ □□ □□ □□□ □□□□ □□ □□□□.
D. □□□□□ □□□ □□□ □□□□ □□ □□□□.
Answer: D (LEAVE A REPLY)

The absence of a right-to-audit clause in the outsourcing contract for a cloud service provider would be of greatest concern to an IS auditor1. This clause gives the client the right to audit the service provider's activities that are relevant to the services being provided1. It is crucial for ensuring that the service provider is complying with the terms of the contract and meeting the client's standards for performance, security, and other aspects1. Without this clause, the client may not be able to effectively monitor and manage risks associated with the outsourcing arrangement1.
References:
Audit rights in outsourcing: certifications and third party reports

NEW QUESTION: 460
□□ □□□ □□□ □□□ □□ □□□ □□□ □ 24□□ □□□ □□ □□□ □□□□□ □□□□□. □□ □ IS □□□□ □□ □□□ □□□□ □□ □□ □□ □□□□ □□ □□ □□□?
A. □□ □□□ □□□ □□□□ □□ □□ □□ □□(KPIs)□ □□□□□.
B. □□ □□□ □□ □□ □□ □□ □□ □□□□ □□□□□.
C. □□ □□ □□□(IDS)□ □□ □□□ □□□□□□.
D. □□ □□ □□ □□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best recommendation for the IS auditor to facilitate compliance with the new regulation is to include the requirement in the incident management response plan. An incident management response plan is a document that defines the roles, responsibilities, processes, and procedures for responding to security incidents. By including the new regulation in the plan, the IS auditor can ensure that the organization is aware of the reporting obligation, has a clear workflow for notifying the regulator within 24 hours, and has the necessary documentation and evidence to support the report.
The other options are not as effective as including the requirement in the incident management response plan:
* Establishing key performance indicators (KPIs) for timely identification of security incidents is a good practice, but it does not guarantee compliance with the regulation. KPIs are metrics that measure the performance of a process or activity, but they do not specify how to perform it. The IS auditor should also provide guidance on how to identify and report security incidents within 24 hours.
* Engaging an external security incident response expert for incident handling is a possible option, but it may not be feasible or cost-effective. The organization may not have the budget or time to hire an external expert, or may prefer to handle the incidents internally. The IS auditor should also evaluate the qualifications and trustworthiness of the external expert, and ensure that they comply with the regulation and other contractual or legal obligations.
* Enhancing the alert functionality of the intrusion detection system (IDS) is a useful measure, but it is not sufficient to comply with the regulation. An IDS is a tool that monitors

network traffic for malicious activity and alerts the network administrator or takes preventive action. However, an IDS may not detect all types of security incidents, or may generate false positives or negatives. The IS auditor should also consider other sources of incident detection, such as logs, reports, audits, or user feedback.

NEW QUESTION: 461
□□ □ □□ □□ □ □□□ □□□□ □□ □ □□□□ □□ □□□□□?
A. □□ □□
B. □□ □□ □□□
C. □□ □
D. □□□ □□
Answer: C (LEAVE A REPLY)
The best assurance of data integrity after file transfers is hash values. Hash values are unique strings that are generated by applying a mathematical function to the data. Hash values can be used to verify that the data has not been altered or corrupted during the transfer, as any change in the data would result in a different hash value. By comparing the hash values of the source and destination files, one can confirm that the data is identical and intact.
The other options are not as effective as hash values for ensuring data integrity after file transfers. Check digits are digits added to a number to detect errors in data entry or transmission, but they are not reliable for detecting intentional or complex modifications of the data. Monetary unit sampling is a statistical sampling technique used for auditing financial statements, but it is not applicable for verifying data integrity after file transfers. Reasonableness check is a validation method that checks whether the data falls within an expected range or format, but it does not guarantee that the data is accurate or consistent with the source.
References:
* 5: On Windows, how to check that data is unchanged after copying? - Super User
* 6: Data integrity | Cloud Storage Transfer Service Documentation | Google Cloud
* 7: Checking File Integrity - HECC Knowledge Base
* 8: How to setup File Transfer Integrity Checks - Progress.com

NEW QUESTION: 462
IS □□□□ □□□□□□ □□□□ □□ □ □□□ □□□□□ □□□□□□□. □□ □ □□ □□ □□□□ □□□□ □□□□□□?
A. □□□□ □□□ □□ □□□□ □□ □□□ □□□□□□.
B. □□□□ □□ □□□ □□ □□□ □□□□□□.
C. □□□□ □□ □□ □□ □□□□ □□ □□□□ □□□□□□.
D. □□□□ □□□ □□ □□□□□ □□□ □□ □□□ □□□□□□.
Answer: (SHOW ANSWER)

The auditor implemented a specific control during the development of the system. This would impair the auditor's independence, as it would create a self-review threat, which is a situation where an auditor has to evaluate or review the results of his or her own work or judgment1. A self-review threat may compromise the auditor's objectivity and impartiality, as the auditor may be biased or influenced by his or her own involvement or interest in the system1. The auditor may also face a conflict of interest or a loss of credibility if he or she has to report on any issues or deficiencies related to the control he or she implemented.

NEW QUESTION: 463
IT □□□□ □□□ □□□ □ IS □□□□ □□□ □□ □□ □ □□□□ □□ □□□□.
A. IT □□ □□□ □□ □□□□□ □□□□ □□□□□.
B. □□□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□□.
C. □□□□ □□□ □□ □□□□□□ □□ □□□ □□□□.
D. □□ □□ □□(KPI)□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 464
□□ □□□ □□ □□ □□□ □□□□□ □□ □ □□ □□□ □□ □□□□?
A. □□ □□
B. □□ □□ □□□
C. 2□□ □□ □□
D. □□□ □□ □□ □□
Answer: (SHOW ANSWER)
The best method to prevent wire transfer fraud by bank employees is system-enforced dual control. System- enforced dual control is a segregation of duties control that requires two or more individuals to perform or authorize a transaction or activity using a system that enforces this requirement. System-enforced dual control can prevent wire transfer fraud by requiring independent verification and approval of payment requests, amounts, and recipients by different bank employees using a system that does not allow any single employee to complete the transaction alone. The other options are not as effective as system-enforced dual control in preventing wire transfer fraud, as they do not involve independent checks or approvals using a system.
Independent reconciliation is a detective control that can help compare and confirm payment records with bank statements, but it does not prevent wire transfer fraud from occurring. Re-keying of wire dollar amounts is an input control that can help detect any errors or discrepancies in payment amounts, but it does not prevent wire transfer fraud from occurring. Two-factor authentication control is an access control that can help verify the identity and authorization of bank employees, but it does not prevent wire transfer fraud from occurring. References: CISA Review Manual (DigitalVersion), Chapter 3, Section 3.2

NEW QUESTION: 465

□□□ □□□□□ □□ □□□□□ □□□ □ IS □□□□ □□□ □□□□□ □□□ □□ □□ □□ □□ □□□ □□□ □□□□ □□□□.

A. □□□ □□

B. □□□□ □□

C. □□□□□(RFP)

D. IT □□□□ □□

Answer: B (LEAVE A REPLY)

The best way for an IS auditor to understand the software benefits to the organization would be to review the business case, which is a document that provides the justification and rationale for acquiring a software solution based on its expected costs, benefits, risks, and alignment with the organization's goals and strategies. The business case helps to evaluate the feasibility and viability of the software acquisition and to support the decision-making process. A feasibility study is a document that analyzes the technical, operational, economic, legal, and social aspects of a software solution to determine its feasibility and suitability for the organization's needs, but it does not necessarily provide a clear indication of the software benefits to the organization. A request for proposal (RFP) is a document that solicits proposals from potential vendors or suppliers for a software solution based on the organization's requirements and specifications, but it does not necessarily provide a clear indication of the software benefits to the organization. The alignment with IT strategy is a factor that influences the software acquisition processand ensures that the software solution supports and enables the organization's IT strategy, but it is not a document that can be reviewed by an IS auditor to understand the software benefits to the organization.
References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.1:
Business Case Development

NEW QUESTION: 466

□□□□ □□ □□ □□□□□ □□□ □ □□ □□□ □□ □□□□□?

A. □□ □□□ □□ □□ □□□□□□.

B. □□□□□ □□ □□ □□□ □□□□□□□.

C. □□ □□ □□□□□ □□□□ □□□□ □□□□ □□□□.

D. □□ □□□ □□ □ □□□□□.

Answer: B (LEAVE A REPLY)

The most important factor to ensure when developing an effective security awareness program is B. Outcome metrics for the program are established. This is because outcome metrics are measures that evaluate the impact and results of the security awareness program on the behavior and performance of the users, and the security posture and objectives of the organization1. Outcome metrics can help ensure the effectiveness of the security awareness program by:

Providing feedback and evidence on whether the security awareness program is achieving its goals and expectations, such as reducing the number of incidents, improving the compliance rate, or increasing the reporting rate1.
Identifying and quantifying the strengths and weaknesses of the security awareness program, and enabling continuous improvement and optimization of the program content, delivery, and frequency1.
Demonstrating and communicating the value and return on investment of the security awareness program to the stakeholders and management, and securing their support and commitment for the program1.

NEW QUESTION: 467
□□□□ □□ □ □ □□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□ □ □ □□□ □□□□ □□□ □□□□. □ □□, □□□ □□ □□□ □ □□ □□□ □□ □ □ □□□ □□□□ □□□□□□. □□ □□ □□□ □□□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
The approach adopted by management in this scenario is risk avoidance. Risk avoidance is the elimination of a risk by discontinuing or not undertaking an activity that poses a threat to the organization3. By moving data center operations to another facility on higher ground, management is avoiding the potential flooding risk that could disrupt or damage the data center. Risk transfer, risk acceptance and risk reduction are other possible approaches for dealing with risks, but they do not apply in this case. References:
* CISA Review Manual, 27th Edition, page 641
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 468
□□□□ □□□ □□ □□(DLP) □□□□ □□□□ □□ □□ □ □□ □□ □□□□ □□ □□□ □□□□□?
A. □□□ □□
B. □□ □□ □□

C. □□ □□□ □□□
D. □□ □□□□ □□
Answer: (SHOW ANSWER)
Configuring rule sets is the first activity that should be completed during the implementation of a DLP solution, because rule sets define the criteria and actions for identifying, monitoring, and preventingdata loss incidents12. Rule sets are based on the organization's data classification, policies, and requirements, and they help to ensure that the DLP solution is aligned with the business objectives and risk appetite34. Configuring rule sets before enabling detection points, establishing exceptions workflow, or configuring reports helps to avoid false positives, false negatives, or unnecessary alerts5.
References
1: 3.13: Deploy a Data Loss Prevention Solution - Read the Docs
2: Plan and implement data loss prevention (DLP) [Guided] - NICCS
3: CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM DATA PROTECTION ... - CISA
4: Continuous Diagnostics and Mitigation Program Technical ... - CISA
5: Data Loss Prevention Best Practices - ISACA Journal

NEW QUESTION: 469
□□□ □□ □□ □□ □□□□□ □□□□ □□□ □□□ □ IS □□□□ □□□□ □ □ □ □□□ □□□ □□□□□?
A. □□□□ □3□□ □□□ □□ □□□ □□□ □□□□ □□□□□.
B. □□□□ □□ □□ □□□ □□□□□.
C. □□□□ □□□ □□□□□ □□ □□□□ □□□ □□□□□.
D. □□□□ □□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□□□□□.
Answer: D (LEAVE A REPLY)
The overall effectiveness of an organization's disaster recovery planning process depends on how well the plan reflects the current and future needs and risks of the organization, and how well the plan is tested, communicated, and maintained. Among the four options given, the most important one for the IS auditor to verify is that management reviews and updates the plan annually or as changes occur.
A disaster recovery plan is not a static document that can be created once and forgotten. It is a dynamic and evolving process that requires regular review and update to ensure that it remains relevant, accurate, and effective. A disaster recovery plan should be reviewed and updated at least annually, or whenever there are significant changes in the organization's structure, operations, environment, or regulations. These changes could affect the business impact analysis, risk assessment, recovery objectives, recovery strategies, roles and responsibilities, or resources of the disaster recovery plan. If the plan is not updated to reflect these changes, it could become obsolete, incomplete, or inconsistent, and fail to meet the organization's recovery needs or expectations.

The other three options are not as important as reviewing and updating the plan, although they may also contribute to the effectiveness of the disaster recovery planning process. Contracting with a third party for warm site services is a possible recovery strategy that involves using a partially equipped facility that can be quickly activated in case of a disaster. However, this strategy may not be suitable or sufficient for every organization or scenario, and it does not guarantee the success of the disaster recovery plan. Scheduling an annual tabletop exercise is a good practice that involves simulating a disaster scenario and testing the plan in a hypothetical setting. However, this exercise may not be enough to evaluate the feasibility or readiness of the plan, and it should be complemented by other types of tests, such as walkthroughs, drills, or full-scale exercises. Documenting and distributing a copy of the plan to all personnel is an essential step that ensures that everyone involved in or affected by the plan is aware of their roles and responsibilities, and has access to the relevant information and instructions. However, this step alone does not ensure that the plan is understood or followed by all personnel, and it should be accompanied by proper training, education, and awareness programs.
Therefore, reviewing and updating the plan annually or as changes occur is the best answer.

NEW QUESTION: 470
□□□□ □□□□ □□ □□ □□□ □□□□□ □□□□□□ □□□ □□□ □□□□□ □ □□□ □□ □□□ □□□ □□□ □□□□□. □□□ □□□□ □□□□ □□□ □, □ □□□ □□□ □□ □□□?
A. □□□ □□ □□□□ □□□□□.
B. □□ □□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□□ □□□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 471
IT □□□ □□ □ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□□ □□□ □ □□□ □□ □□□□□.
A. □□ □□ □□(BIA).
B. □□ □ □□ □□.
C. □□ □□□ □□(BCP).
D. □□ □□ □□(DRP).
Answer: C (LEAVE A REPLY)
A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A core part of a BCP is the documentation of workaround processes to keep a business function operational during recovery of IT systems. Workaround processes are alternative methods or procedures that

can be used to perform a business function when the normal IT systems are unavailable or disrupted2. For example, if an online payment system is down, a workaround process could be to accept manual payments or use a backup system. Workaround processes help to minimize the impact of IT disruptions on the business operations and ensure continuity of service to customers and stakeholders3.
References:
* 1 explains what is a business continuity plan and why it is important.
* 2 defines what is a workaround process and how it can be used in a BCP.
* 3 provides examples of workaround processes for different business functions.

NEW QUESTION: 472
□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□□ □ □ IS □□□□ □□ □□ □□ □ □□□ □□□□□?
A. □□□□□ □□□□□□ □ □ □□□□.
B. □□ □□□ □□□ □□□ □ □□□□.
C. □□□ □□ □□□□□□ □□ □□□ □□□ □ □□□□.
D. □□ □□□□ □□ □□□ □□□□ □□ □□ □□□□.
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Thebiggest concernwhen implementing aglobal data privacy policyis thatlocal regulations may contradictthe global policy, leading tolegal and compliance risks.
* Local Regulations May Contradict the Policy (Correct Answer - B)
* Different countries havevarying data privacy laws(e.g.,GDPR in Europe,CCPA in California, PDPA in Singapore).
* A global policy mayconflict with stricter local laws, making compliancechallenging.
* Example:GDPR requiresexplicit consentfor data processing, but other jurisdictions may allowimplied consent.
* Requirements May Become Unreasonable (Incorrect - A)
* Not a primary risk; compliance is more critical.
* Conflicts with Application Requirements (Incorrect - C)
* Applications shouldadapt to regulations, not the other way around.
* Local Management Resistance (Incorrect - D)
* Management acceptance is important but can beaddressed through training.
References:
* ISACA CISA Review Manual
* GDPR (General Data Protection Regulation)
* ISO 27701 (Privacy Information Management System)

NEW QUESTION: 473
□□ □ □□ □□□ □□ □□□ □□□ □□□□ □□ □ □□□□□ □□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□ □ □□ □□□□□?

A. □□ □□□
B. □□ □□□
C. □□□ □□□
D. □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 474
□□□ □□ □□□□□ □□□□□ □□□□ IS □□□□ □□ □□□ □□□ □□ □ □ □□□□?
A. □□□□□ □□□□ □□ □□□□ □□ □□□□ □□ □□
B. □□□□□□ □□□ □□□□ □□
C. □□□□□ □□□□ □□□□ □□□□ □□□□□ □□□□□.
D. □□□ □□ □□ □□ □□
Answer: A (LEAVE A REPLY)
IS auditors primarily provide assurance and oversight. In this context, independent reviews ensure that those responsible for the renovation project are meeting their obligations, following best practices, and managing risks appropriately.
References:
ISACA's Code of Professional Ethics: Emphasizes the IS Auditor's duty to be independent and objective.
The Role of IS Audit: IS Auditors are not project managers but provide objective assessment and guidance regarding controls and risk mitigation within projects.
CISA Review Manual (27th Edition): May have sections discussing the role of IS auditors in infrastructure projects or similar initiatives.

NEW QUESTION: 475
□□ □□□ □□ IS □□□□ □□□□ □□ □□ □□ □□ □□□ □□□ □□ □□ □□ □ □□□□□ □□□□□ □□□ □□ □□□. IS □□□□ □□□□ □□□ □□ □□□ □ □□□□. □□ □ IS □□□□ □□ □□ □□□ □□□□□?
A. □□□□ □□□ □□□□ □□ □□□ □□□□□.
B. IS □□ □□ □□□ □□□ □□□□□.
C. □□□□ □□ □□□ □□□ □□□□□.
D. □□□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Prior to a follow-up engagement, if an IS auditor learns that management has decided to accept a level of residual risk related to an audit finding without remediation, the IS auditor should report the issue to IS audit management. This is because IS audit management is responsible for ensuring that audit findings are properly communicated and resolved. Accepting management's decision and continuing the follow-up would not address the IS auditor's concern. Reporting the disagreement to the board or executive management

would be premature and inappropriate without consulting IS audit management first.
References: CISA Review Manual (Digital Version), Chapter 1, Section 1.6

NEW QUESTION: 476
IS □□□□ □□□□□□ □□ □□□ □□ □□ □□□□ □□ □□□ □□ □□ □□□ □ □□□?
A. □□ □□ □□(BIA)□ □□□□□.
B. □□□ □□□ □□□□□□□ □□□□□.
C. □□ □□□ □□□□□□ □□□ □□□□□.
D. □□□□ □□□□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
The first task that an IS auditor should complete during the preliminary planning phase of a database security review is to determine which databases will be in scope. The scope defines the boundaries and objectives of the audit, as well as the resources, time, and budget required. The IS auditor should identify the databases that are relevant to the audit based on factors such as their criticality, risk, complexity, size, type, location, and ownership. The IS auditor should also consider the regulatory, contractual, and organizational requirements that apply to the databases. By defining the scope clearly and accurately, the IS auditor can ensure that the audit is focused, feasible, and effective.
References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 477
□□□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□ □□ □□□□ □□□□. □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□□ □□□□□.
C. □□ □□□□ □□ □□ □□(NDA)□ □□□□□ □□□□□.
D. □□ □□□ □□□(EUC)□ □□ □□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 478
□□ □□□□□ □□□ □□ □□ □□□ □□□□ □□□ □□ □□(DLP) □□□□ □□ □□ □□□□. □□ □□□□. □□ □ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□ □□□
B. □□□ □□□ □□□ □□
C. □□ □□
D. □□□□□□ □□□□(EA)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 479
□□□ □□ □□(DLP) □□□ □□ □□ □□ □□□ □□□□ IS □□□□ □□ □ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□ □□□ □□□ □□□□□.
B. □□□□ □□□ □□□□ □□□□ □ □□□□□.
C. □□ □□ □□□ □□ □□ □□□ □□□ □□□.
D. □□□ □□ □□□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
A data loss prevention (DLP) tool implemented in monitor mode only observes and logs potential data leakage but does not actively prevent it. This leaves the organization vulnerable to data breaches, making it the most critical concern in a pre-implementation review.
* Crawlers for Sensitive Data (Option B): While crawlers may pose a performance impact, they are essential for discovering sensitive data.
* Deep Packet Inspection (Option C): Though it introduces privacy considerations, it is a standard DLP functionality for inspecting data in transit.
* Encryption Key Management (Option D): While important for security, improper management does not immediately prevent DLP functionality.
Reference: ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 480
□□ □ IT □□ □□□□□□ □□□□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□□□ □□□ □□□ □□□□ □□□ □□□□□□.
B. □□ □□ □□□ □□ □□□□□ □□
C. IT □□ □□ □ □□ □□□
D. □□□□□ □□□ □□□□ □□□□ □□ □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 481
□□ □ □□□ □□ □□□□□ □□□ □□□ □□□□ IS □□□□□ □□ □ □□□□ □ □□ □□ □□□□□?
A. □□ □□ □□□ □□□□ □□□□□.
B. □□□□ □□□ □□ □□□ □□ □□□□.
C. □□□ □□□ □□ □□□ □ □□ □□ □□ □□□ □□□□.
D. □□□ □□ □□□ □□ □□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 482
IS □□□□ □□□ □□□□□ □□ □□ □□ □□□ □□□ □□□□□□.
□□ □ □□ □□ □□□ □□ □□□?
A. □□ □□□□ □□ □□□ □□□□□□.
B. □□□ □□□ □□□ □□□□□.
C. □□□ □□ □□□□□ □□□□□.
D. □□ □□□□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
An IS auditor has identified deficiencies within the organization's software development life cycle (SDLC) policies. The SDLC is the process of planning, developing, testing, and deploying software applications1. SDLC policies are the guidelines and standards that govern the SDLC process and ensure its quality, security, and compliance2. Deficiencies in SDLC policies can lead to various risks, such as:
Software errors, bugs, or vulnerabilities that can affect the functionality, reliability, or security of the applications3 Software failures, delays, or overruns that can affect the delivery, performance, or customer satisfaction of the applications3 Software non-compliance that can result in legal, regulatory, or contractual violations or penalties3 The next step that the IS auditor should do after identifying deficiencies in SDLC policies is to communicate the observation to the auditee. The auditee is the person or entity that is subject to the audit and is responsible for the area being audited4. In this case, the auditee could be the software development manager, the project manager, or the senior management of the organization. Communicating the observation to the auditee is important for several reasons:
It allows the IS auditor to verify the accuracy and validity of the observation and gather additional evidence or information from the auditee4 It gives the auditee an opportunity to respond to the observation and provide their perspective, explanation, or justification for the deficiencies4 It enables the IS auditor to discuss with the auditee the potential impact, root cause, and remediation plan for the deficiencies4 It fosters a collaborative and constructive relationship between the IS auditor and the auditee and promotes transparency and accountability in the audit process4 The other options are not as appropriate as communicating the observation to the auditee. Documenting the findings in the audit report is a later stepthat should be done after communicating with the auditee and finalizing the observation. Identifying who approved the policies is not relevant for addressing the deficiencies and may imply blame or fault on a specific person or group.

Escalating the situation to the lead auditor is not necessary unless there is a serious disagreement or conflict with the auditee that cannot be resolved by normal communication. Therefore, option D is the correct answer.
References:
What Is The Software Development Life Cycle? | PagerDuty
Software Development Life Cycle (SDLC) Policy | StrongDM
What Is SDLC? Best Phases, Methodologies, and Benefits Revealed - Kellton
Communicating Audit Findings

NEW QUESTION: 483
□□ □ □□□ □□□□□□ □□□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□□
D. IT □□□ □□□□
Answer: C (LEAVE A REPLY)
File checksums are values that are calculated from the contents of a file and can detect any changes or corruption in the file. They are used to verify that the files that are transferred or processed through system interfaces are not altered in any way. File checksums are more effective than periodic audits, file counts, or IT operator monitoring, which are other types of controls that can help ensure the integrity of system interfaces, but they are not as reliable or timely as file checksums.

NEW QUESTION: 484
□□ □□□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□ □□□ □□□ □□□ □.
A. □□ □□□ □□□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□ □□□□ □□□□□.
D. □□□□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 485
□□ □□ IS □□ □□□□□ □□□ □ IS □□□□ □□ □□□ □□□ □ □□□ □□□ □□?
A. □□□□□ □□
B. □□ □□
C. □□□□ □□□□
D. IT □□ □□
Answer: C (LEAVE A REPLY)

Business processes should be the primary focus of an IS auditor when developing a risk-based IS audit program, because they represent the core activities and functions of the organization that support its objectives and goals. Business processes also involve the use of IT resources and systems that may pose risks to the organization's performance and compliance. A risk-based IS audit program should identify and assess the risks associated with the business processes and determine the appropriate audit scope and procedures to provide assurance on their effectiveness and efficiency. Portfolio management, business plans, and IT strategic plans are also relevant factors for developing a risk-based IS audit program, but they are not as important as business processes. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.2.1

NEW QUESTION: 486
IS □□□□ □□□ □□ □□□□ □□□(RPA)□ □□□□ □□□□ □□□□ □□□ □ □□□□□ □□□ □□□ □, □□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □ □□□□□ □□□□ □□□□□□.
B. □□ □ □□□□ □□□□□ □□ □□□ □□□ □□□□□.
C. RPA□ □□□□ □□ □□□ □□ □□□□ □□□ □□□□□□□.
D. □□□ □□ □□□□□ □□ □□□(RFP)□ □□□□□□□.
Answer: A (LEAVE A REPLY)
The most important thing for an IS auditor to confirm when reviewing an organization's plans to implement robotic process automation (RPA) to automate routine business tasks is that the end-to-end process is understood and documented. This is because RPA involves the use of software robots or digital workers to mimic human actions and execute predefined rules and workflows. Therefore, it is essential that the IS auditor verifies that the organization has a clear and accurate understanding of the current state of the process, the desired state of the process, the inputs and outputs, the exceptions and errors, the roles and responsibilities, and the performance measures12. Without a properdocumentation of the end-to-end process, the organizationmay face challenges in designing, developing, testing, deploying, and monitoring the RPA solution3. References: 1: CISA ReviewManual (Digital Version), Chapter 4: Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support, page 211 2:CISA Online Review Course, Module 4: Information Systems Operations and Business Resilience, Lesson 4.2: IT Service Delivery and Support 3: ISACA Journal Volume 5, 2019, Article: Robotic Process Automation: Benefits, Risks and Controls

NEW QUESTION: 487
IS □□□□ □□□ □□ □□□□ □□□□□□□ □□ □□□ □□ □□□ □□□□ □□ □□. □□ □ □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□ □□□□□ □□□□□ □□□ □□□ □□□□.
B. □□□□ □□□□□□ □□□ □□ □□□ □□□□ □□□□.
C. □□□ □□□ □□□ □□ □□□□□.

D. □□□□ □□□ 8□□ □□□□□□□.

Answer: C (LEAVE A REPLY)

The finding that should be of greatest concern to the IS auditor is that user accounts are shared between users.

User accounts are unique identifiers that grant access to an organization's financial business application based on the roles and responsibilities of the users. User accounts should be individualized and personalized to ensure accountability, traceability, and auditability of user actions and transactions. User accounts should not be shared between users, because this can compromise the confidentiality, integrity, and availability of the financial data and systems, and can enable unauthorized or fraudulent activities. If user accounts are shared between users, the IS auditor may not be able to determine who performed what action or transaction, or whether the user had the appropriate authorization or approval. The other findings are also concerning, but not as much as user account sharing, because they either affect the password strength or frequency rather than the useridentity, or they relate to monitoring rather than controlling user access.

References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.2

NEW QUESTION: 488

□□□□ □□□□□ □□ □□ □□□ □□□ □□□ □□ □□□ IT □ □□ □□□ □□ IS □□□□□ □□ □□ □□ □□□ □□□ □□□□.

A. □□□□□□□ □□□□□□□ □□□ □□ □□□ □□□□□.

B. □□□□ □□□□ □□□ □□□□□.

C. □□□□□ □□□□ □□□ □□□ □□□□□.

D. □□□□ □□ □□□ □□□ □□ □□

Answer: C (LEAVE A REPLY)

The best recommendation for a small IT web development company where developers must have write access to production is to remove production access from the developers. Production access is the ability to modify or update the live systems or applications that are used by customers or end users. Production access should be restricted to authorized and qualified personnel only, as any changes or errors in production can affect the functionality, performance, or security of the systems or applications. Developers should not have write access to production, as they may introduce bugs,vulnerabilities, or inconsistencies in the code that can compromise the quality or reliability of the systems or applications. The other options are not as effective as removing production access from the developers, as they do not address the root cause of the problem or provide the same benefits. Hiring another person to perform migration to production is a costly solution that can help segregate the roles and responsibilities of developers and migrators, but it does not remove production access from the developers. Implementing continuous monitoring controls is a good practice that can help detect and correct any issues or anomalies in production, but it does not remove production access from the developers. Performing a user access review for the development team is a detective control that can help verify and

validate the access rights and privileges of developers, but it does not remove production access from the developers. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 489
IS □□□□ IT □□ □□□□□ □□□□ □□ □□□ □□□□□□□□(PDCA) □□□ □□□□ □□□□ □ □□□ □□□ □□□□ □□□□□ □□□. □ □□□□ □□□□ PDCA □□□□□ □□ □□ □ □□ □□□ □□ □□□□ □□□?
A. □□
B. □□
C. □□□
D. □□
Answer: B (LEAVE A REPLY)
In the PDCA cycle, the "Plan" phase is where targets and objectives are defined. Focusing on this phase allows the auditor to evaluate the accuracy and appropriateness of the defined targets before they are implemented and measured in subsequent phases.
References
* ISACA CISA Review Manual 27th Edition, Page 315-316 (PDCA Cycle)

NEW QUESTION: 490
□□ □ □□ □□□ □□□□□?
A. □□ □□, □□□, □□ □□
B. □□□ □□□□ □□ □□ □□
C. □□□ □□ □□□ □□ □□ □□
D. □□ □□ □□ □□
Answer: D (LEAVE A REPLY)
A corrective control is a control that aims to restore normal operations after a disruption or incident has occurred. Executing emergency response plans is an example of a corrective control, as it helps to mitigate the impact of an incident and resume business functions.
Separating equipment development testing and production is a preventive control, as it helps to avoid errors or unauthorized changes in production systems.
Verifying duplicate calculations in data processing is a detective control, as it helps to identify errors or anomalies in data processing. Reviewing user access rights for segregation is also a detective control, as it helps to detect any violations of segregation of duties principles. References: ISACA, CISA Review Manual,
27th Edition, 2018, page 64

NEW QUESTION: 491
□□□ □□□□□□ □□□□ □□□□ □□ □□□ □□ □ □□□□□□□ □□□□ |$ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□□□□ □□□□□ □□□□□ □□□□□.

B. □□ □□□ □ □□□□ □□□ □□□□□ □□□ □ □□□□.
C. □□ □ □□□□ □□ □□□ □□□ □□□□□□.
D. □□□ □□□ □□ □□□□□ □□□□ □□□□□□□.
Answer: C (LEAVE A REPLY)
The finding that should be of greatest concern to an IS auditor reviewing data conversion and migration during the implementation of a new application system is that unauthorized data modifications occurred during conversion. Data conversion and migration is a process that involves transferring data from one system to another, ensuring its accuracy, completeness, integrity, and usability. Unauthorized data modifications during conversion can result in data loss, corruption, inconsistency, or duplication, which can affect the functionality, performance, reliability, and security of the new system. Unauthorized data modifications can also have serious business implications, such as affecting decision making, reporting, compliance, customer service, and revenue. The IS auditor should verify that adequate controls are in place to prevent, detect, and correct unauthorized data modifications during conversion, such as access control, data validation, reconciliation, audit trail, and backup and recovery. The other findings (A, B and D) are less concerning, as they can be mitigated by documenting the change management process, restoring the backups of the old system and data from offline storage, or automating the data conversion process. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.4: System Implementation

NEW QUESTION: 492
IS □□□□ □□ □□□ □□ □□ □□(SDLC) □□□□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□□□. □□□□ □□ □□ □□ □ □□ □□□ □□ □□□ □□□ □ □□□?
A. □□ □□
B. □□□ □□ □□
C. □□ □□(QA) □□
D. □□ □□
Answer: C (LEAVE A REPLY)
The quality assurance (QA) phase is the phase where the IS auditor should first examine requirements from an in-house SDLC project that has not met user specifications. This is because the QA phase is the phase where the system is tested and verified against the user specifications and the design specifications to ensure that it meets the functional and non-functional requirements, as well as the quality standards and expectations. The QA phase involves various testing activities, such as unit testing, integration testing, system testing, acceptance testing, performance testing, security testing, etc., to identify and resolve any defects, errors, or deviations from the specifications12.
The configuration phase is not the phase where the IS auditor should first examine requirements from an in- house SDLC project that has not met user specifications. The configuration phase is the phase where the system is installed and configured on the target

environment, such as hardware, software, network, etc., to prepare it for deployment and operation. The configuration phase may involve activities such as installation, customization, migration, integration, etc., to ensure that the system is compatible and interoperable with the existinginfrastructure and systems34.
The user training phase is not the phase where the IS auditor should first examine requirements from an in- house SDLC project that has not met user specifications. The user training phase is the phase where the end- users are trained and educated on how to use the system effectively and efficiently. The user training phase may involve activities such as developing training materials, conducting training sessions, providing feedback and support, etc., to ensure that the users are familiar and comfortable with the system features and functions56.
The development phase is not the phase where the IS auditor should first examine requirements from an in- house SDLC project that has not met user specifications. The development phase is the phase where the system is coded and built based on the design specifications and the user specifications. The development phase may involve activities such as programming, debugging, documenting, etc., to create a working prototype or a final product of the system

NEW QUESTION: 493
IS □□□□ □□ □□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□ □?
A. □□□ □□□□ □□□□□□
B. □□□□ □□□□
C. □□ IT □□
D. □□ □□ □□
Answer: (SHOW ANSWER)
This is because the business processes are the core activities and functions that enable the organization to achieve its objectives and create value for its stakeholders. The business processes are also the sources and drivers of various risks that may affect the organization's performance, compliance, and reputation. Therefore, the IS auditor should focus on understanding, assessing, and prioritizing the business processes that are most critical, complex, or vulnerable to the organization's success, and align the audit objectives, scope, and resources accordingly12.
Critical business applications (A) are not the most important area of focus for an IS auditor when developing a risk-based audit strategy, but rather a specific aspect of the business processes that may require attention.
Critical business applications are the software systems that support the execution and automation of the business processes, such as enterprise resource planning (ERP), customer relationship management (CRM), or accounting systems. Critical business applications may pose significant risks to the organization if they are not reliable, secure, or efficient. Therefore, the IS auditor should consider the criticality, functionality, and

dependency of the business applications when planning the audit, but not as the primary focus12.
Existing IT controls are not the most important area of focus for an IS auditor when developing a risk- based audit strategy, but rather an outcome or output of the risk assessment process. Existing IT controls are the policies, procedures, practices, and technologies that are implemented to manage and mitigate the IT- related risks that may affect the organization's business processes and objectives. Existing IT controls may vary in their design, effectiveness, and maturity. Therefore, the IS auditor should evaluate and test the existing IT controls as part of the audit execution and reporting process, but not as the main focus12.
Recent audit results (D) are not the most important area of focus for an IS auditor when developing a risk- based audit strategy, but rather an input or source of information for the risk assessment process. Recent audit results are the findings, recommendations, and opinions of previous audits that may provide insights or feedback on the organization's business processes, risks, and controls. Recent audit results may also indicate any changes or trends in the organization's risk profile or environment. Therefore, the IS auditor should review and consider the recent audit results as part of the audit planning and scoping process, but not as the main focus12.

NEW QUESTION: 494
IS □□□□ □□□ □□□ IT □□ □□ □□□□□□ □□ □ □□ □□□ □□□ □□□.
□□ □ □□ □□□ □□□□ □□ □□ □□□ □□□?
A. IT □□ □□□
B. □□□ □□ □□(SLA)
C. □□□□ □□□□□ □□
D. □□□□□□ □□□□(EA)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 495
□□ □□□□ □□□ □□□ □□ □□□ □□□□ □ □□ □□□ □□ □□□ □□ □ □ □□□□?
A. □□□ □□ □□ □ □□
B. □□□ □□ □□□ □□ □□
C. □□ □□□ □□ □□ □□□
D. □□ □□ □□ □ □□□□ □□ □□
Answer: A (LEAVE A REPLY)
The best source of information to determine the required level of data protection on a file server is the data classification policy and procedures, which define the criteria and methods for classifying data according to its sensitivity, value, and criticality, and specify the appropriate security measures and controls for each data category. Data classification policy and procedures help to ensure that data is protected in proportion to its importance

and risk exposure. Access rights of similar file servers, previous data breach incident reports, and acceptable use policy and privacy statements are not sufficient or reliable sources of information to determine the required level of data protection on a file server, as they do not provide clear and consistent guidance on how to classify and protect data. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Information Asset Security Framework

NEW QUESTION: 496
□□ □□□ □□□ □ □□ □□□ □□□□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□□ □□□□ □□□ □□□□ □□
B. □□ □□□ □□□ □□□□ □□□□□ □□ □□□ □□□□□.
C. □□ □□ □□ □□ □□□□ □□□ □□□ □ □□□ □□□□.
D. □□ □□□ □□□ □□□□□ □□□ □□□ □□□ □ □□□ □□□.
Answer: B (LEAVE A REPLY)
The primary purpose of documenting audit objectives when preparing for an engagement is to identify areas with relatively high probability of material problems. Audit objectives are statements that describe what the audit intends to accomplish or verify during the engagement. Audit objectives help the IS auditor to focus on the key areas of risk or concern, to design appropriate audit procedures and tests, and to evaluate audit evidence and results. By documenting audit objectives, the IS auditor can identify areas with relatively high probability of material problems that may affect the achievement of audit goals or business objectives.
Addressing the overall risk associated with the activity under review, ensuring maximum use of audit resources during the engagement and prioritizing and scheduling auditee meetings are also purposes of documenting audit objectives, but they are not as primary as identifying areas with high probability of material problems. References:
* CISA Review Manual, 27th Edition, page 1111
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 497
□□ □ □□□□□□ □□□□(EA) □□□□□ □□ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□ □□□□□ □□□ □□□□ □□□□□.
B. EA□ □□□ □□ □□□ □□□ □ □□□ □□□□□.

C. EA□ □□ □□ □ □□□ □□□□□ □□□□□.
D. □□□ □□□□□□ □□ □□□ □□ □□□(ROI)□ □ □ □□□ □□□□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:Enterprise architecture (EA) governance ensures that IT and business alignment is maintained and that new processes and technologies integrate well with existing structures.
* Option A (Correct):The primary purpose of EA governance is to ensure that new technologies, processes, and systems align and harmonize with existing architecture to maintain operational efficiency and consistency.
* Option B (Incorrect):While adaptability to emerging technology trends is important, EA governance focuses more on structure, consistency, and compliance rather than just adaptability.
* Option C (Incorrect):Compliance with regulations is crucial, but it is just one component of governance.
EA governance has a broader scope, including strategic alignment and process integration.
* Option D (Incorrect):Ensuring ROI is an important financial consideration, but it is not themainobjective of EA governance.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Covers governance, risk management, and ensuring alignment of EA with business objectives.

NEW QUESTION: 498
□□ □ IT □□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□ □□
B. □□ □□□ □□□ □□ □□
C. □□□ □□ □ 0t
D. □□□ □□ □
Answer: (SHOW ANSWER)
The answer D is correct because the number of reopened tickets is the best indicator for measuring the performance of IT help desk function. Reopened tickets are tickets that have been marked as resolved by the help desk agents, but the customers are not satisfied with the resolution and reopen them for further assistance. Reopened tickets reflect the quality and effectiveness of the help desk service, as well as the customer satisfaction level. A high number of reopened tickets indicates that the help desk agents are not resolving the issues properly, or that they are not communicating well with the customers. This can lead to customer frustration, dissatisfaction, and churn. Therefore, minimizing the number of reopened tickets is a key goal for any help desk function.
The other options are not as good as option D. Percentage of problems raised from incidents (option A) is a metric that shows how many incidents are escalated to problems, which are more complex and require root cause analysis and long-term solutions. This

metric reflects the complexity and severity of the issues faced by the customers, but it does not directly measure the performance of the help desk function. Mean time to categorize tickets (option B) is a metric that shows how long it takes for the help desk agents to assign a category to each ticket, such as technical, billing, or feedback. This metric reflects the efficiency and accuracy of the help desk agents, but it does not measure the quality or effectiveness of the resolution. Number of incidents reported (option C) is a metric that shows how many issues are reported by the customers to the help desk function. This metric reflects the demand and workload of the help desk function, but it does not measure how well the issues are resolved or how satisfied the customers are.
References:
* Key Metrics to Measure Help Desk Performance
* 8 service desk KPIs and performance metrics for IT support
* 13 Most Important Help Desk KPIs to Track and Measure Help Desk Performance

NEW QUESTION: 499
□□ □□ □ IS □□□□ □□ □□□ □□□□□.
□□□ □□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□ □□□□. □□ □ □□ □□ □□□ □□□□□?
□□□□ □□ □□□ □□□□□ □□□?
A. □□ □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□ □□□ □□□ □□□□□.
C. □□ □□□ □□□ □□□ □□□□□.
D. □□ □□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The best way to help management understand the associated risk of missing backup cycles due to operator error and lack of exception management is to explain the impact to disaster recovery. Disaster recovery is the process of restoring normal operations and functions after a disruptive event, such as a natural disaster, a cyberattack, or a hardware failure. Backup cycles are essential for disaster recovery, because they ensure that the organization has copies of its critical data and systems that can be restored in case of data loss or corruption. If backup cycles are missed due to operator error, and these exceptions are not managed, the organization may not have the latest or complete backups available for disaster recovery, which can result in prolonged downtime, reduced productivity, lost revenue, reputational damage, and legal or regulatory penalties. The other options are not as effective as explaining the impact to disaster recovery, because they either do not address the risk of data loss or corruption, or they focus on operational or technical aspects rather than business outcomes. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

NEW QUESTION: 500
□□ □ □□□ □□□ □□□□□ □□ □□ □□□ □□□□□?

A. □ □ □□ □□□ □□□□□
B. □□□ □□□□ □□□□□.
C. □□□ □□□□ □□□□□.
D. □□ □□□ □□ □□
Answer: B (LEAVE A REPLY)
Sampling risk is the risk that the auditor's conclusion based on a sample may be different from the conclusion that would be reached if the entire population was tested using the same audit procedure. Sampling risk can lead to either incorrect rejection or incorrect acceptance of the audit objective. The best way to minimize sampling risk is to perform statistical sampling. Statistical sampling is a method of selecting and evaluating a sample using probability theory and mathematical calculations. Statistical sampling allows auditors to measure and control the sampling risk by determining the appropriate sample size and selection method, and evaluating the results using confidence levels and precision intervals. Statistical sampling can also provide more objective and consistent results than judgmental sampling, which relies on the auditor's professional judgment and experience.
References:
* 6: Sampling Risks: Definition, Example, and Explanation - Wikiaccounting
* 7: Sampling Risk in Audit | Sampling vs non sampling risk - Accountinguide
* 9: Audit sampling | ACCA Qualification | Students | ACCA Global

NEW QUESTION: 501
□□ □□□ □□□□ □□ □□ □□ □□ □□ □ □□ □□□ □□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
When storage space is limited,incremental backupsare the most efficient because they store only the changes made since the last backup, reducing storage requirements.
* Option A (Correct):Incremental backupsonly store data that has changed since the last backup, significantly reducing storage usage while maintaining a historical record of changes.
* Option B (Incorrect):Mirror backupscreate an exact copy of the entire system, consuming significant storage space andnot retaining historical versions.
* Option C (Incorrect):Full backupscapture everything and require large amounts of storage, making them impractical for space-constrained environments.
* Option D (Incorrect):Annual backupsrefer to frequency rather than method. They do not inherently optimize storage usage.

Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Covers backup strategies, storage management, and disaster recovery.

NEW QUESTION: 502
□□ □□□□□ □□□ □□□ □□□□□ □ □□□ □□□□ □□□. □□□ □ □□□ □□ □□ □□□ □□□ □□□ □□□□□□□. □□ □□□ □□□ □□□□□□□?
A. □□
B. □□□
C. □□
D. □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 503
□□ □ □□□ □□□□□□ □□□ □□□□ □□ □□ □□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□□ □□□□ □□□□□
B. □□□ □□ □□□□□ □□□□
C. □□□□ □□□□□ □□□□
D. □□□ □□ □□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 504
□□ □ □□ □□□ □□□ □□ □□ □ IS □□□□ □□ □□□□ □ □□ □□□□□?
A. □□□ □□□□ □□□ □□□ □□ □□ □□□□.
B. □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□□□.
C. □□ □□□ □□□□□ □□□ □□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□□□□ □□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 505
□□ □ □3□ □□□□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□□□ □□ □□□□ □□
B. □□□□□ □□□ □□ □□ □□□ □□
C. □□□□□ □□ □□□□ □□□□ □□
D. □□□□ □□□□ □□□□ □□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 506
□□□ □□ □□□□□ □□ □□ □□□□ □□ □□ □ □□ □□ □□□□□?

A. □□ □□
B. □□ □□
C. □□□□□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)
Impact assessment is an activity that occurs during the issues management process for a system development project. Issues management is a process of identifying, analyzing, resolving, and monitoring issues that may affect the project scope, schedule, budget, or quality. Impact assessment is a technique of evaluating the severity and priority of an issue, as well as its implications for the project objectives and deliverables. The other options are not activities that occur during the issues management process, but rather related to other processes such as contingency planning, configuration management, or help desk management. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.3.31
* CISA Review Questions, Answers & Explanations Database, Question ID 217

NEW QUESTION: 507
□□□□ □□ □ □□ □ □□ □□□ □□□□□?
A. □□ □□ □□□□ □□□□ □□□□□.
B. □□ □□□□ □□□□ □□□ □□□□ □□□□□.
C. □□ □□□□ □□ □□□ □□□□ □□□□□.
D. □□□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 508
□□ □ □□□ □□□□□ □□ □□□□ □□□ □□□□ □□□□ □ □□□□ □□ □ □ □□ □□□□□?
A. □□□□ □□□□ □□□□□ □□ □□ □□□
B. □□□□ □□□□ □□
C. □□□□ □□□□□ □□□□□ □□
D. □□□ □□□ □□ □□□□□
Answer: D (LEAVE A REPLY)
A project deliverable is a tangible or intangible product or service that is produced as a result of a project and delivered to the customer or stakeholder. A project deliverable can be either an intermediate deliverable that is part of the project process or a final deliverable that is the outcome of the project.
An agile software development methodology is a project management approach that involves breaking the project into phases and emphasizes continuous collaboration and improvement. Teams follow a cycle of planning, executing, and evaluating. Agile software development methodologies value working software over comprehensive documentation and respond to change over following a plan.

Rapidly created working prototypes are most likely to be a project deliverable of an agile software development methodology because they:
Provide early and frequent feedback from customers and stakeholders on the functionality and usability of the software product Allow for rapid validation and verification of the software requirements and design Enable continuous improvement and adaptation of the software product based on changing customer needs and expectations Reduce the risk of delivering a software product that does not meet customer needs or expectations Increase customer satisfaction and trust by delivering working software products frequently and consistently Some examples of agile software development methodologies that use rapidly created working prototypes as project deliverables are:
Scrum - a framework that organizes the work into fixed-length sprints (usually 2-4 weeks) and delivers potentially shippable increments of the software product at the end of each sprint1 Extreme Programming (XP) - a methodology that focuses on delivering high-quality software products through practices such as test-driven development, pair programming, continuous integration, and frequent releases2 Rapid Application Development (RAD) - a methodology that emphasizes rapid prototyping and user involvement throughout the software development process3 The other options are not likely to be project deliverables of an agile software development methodology.
Strictly managed software requirements baselines are not likely to be project deliverables of an agile software development methodology. A software requirements baseline is a set of agreed-upon and approved software requirements that serve as the basis for the software design, development, testing, and delivery. A strictly managed software requirements baseline is a software requirements baseline that is controlled and changed only through a formalchange management process. Strictly managed software requirements baselines are more suitable for traditional or waterfall software development methodologies that follow a linear and sequential process of defining, designing, developing, testing, and delivering software products. Strictly managed software requirements baselines are not compatible with agile software development methodologies that embrace change and flexibility in the software requirements based on customer feedback and evolving needs.
Extensive project documentation is not likely to be project deliverables of an agile software development methodology. Project documentation is any written or electronic information that describes or records the activities, processes, results, or decisions of a project. Extensive project documentation is project documentation that covers every aspect of the project in detail and requires significant time and effort to produce and maintain. Extensive project documentation is more suitable for traditional or waterfall software development methodologies that rely on comprehensive documentation to communicate and document the project scope, requirements, design, testing, and delivery. Extensive project documentation is not compatible with agile software development methodologies that value working software over comprehensive documentation and use minimal documentation to support the communication and collaboration among the project team members.

Automated software programming routines are not likely to be project deliverables of an agile software development methodology. Automated software programming routines are programs or scripts that perform repetitive or complex tasks in the software development process without human intervention. Automated software programming routines can improve the efficiency, quality, and consistency of the software development process by reducing human errors, saving time, and enforcing standards. Automated software programming routines can be used in any software development methodology, but they are not specific to agile software development methodologies. Automated software programming routines are not considered as project deliverables because they are not part of the final product that is delivered to the customer.

NEW QUESTION: 509
□ □□□ □□□ □ □□ □□□□ □□□□□□ □□□□ □□□ □ □ □ □, □□□□ □ □ □□ □□□ □□□ □□□ □□□□□. □□ □□□□ □□ □□□ □□□ □□□□.
A. □□ □□□□ □□ □□□□ □□□□□□ □□□□□.
B. □□□ □□□□ □□□□□□ □□□ □□ □□ □□□□ □□□□□.
C. □□□□ □□ □□□□ □□□□□□ □□ □□□□□.
D. □□ □□□ □□□□ □□□ □ □□ □□□□ □□□□□□□ □□ □□□□ □□□□ □.
Answer: D (LEAVE A REPLY)
Using analytical tools to produce exception reports from the system and performance monitoring software is the most effective plan of action for a company that purchased and implemented system and performance monitoring software. Exception reports are reports that highlight deviations or anomalies from predefined thresholds or standards. Using analytical tools to produce exception reports can help to reduce the size and complexity of the system and performance monitoring reports, as well as to focus on the most relevant and critical information for review and action. The other options are less effective plans of action, as they may involve unnecessary costs, risks, or efforts. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
* CISA Review Questions, Answers & Explanations Database, Question ID 219

NEW QUESTION: 510
□□ □□ □ □□ □□□ IT □□ □□ □□ □□□ □□□ □□□□ □□□?
A. □□□□
B. □□ □□ □□
C. □□□
D. □□ □□ □□
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Theaudit charteris a formal document that definesthe purpose, authority, and responsibilitiesof the internal audit function.

* Audit Charter (Correct Answer - A)
* Establishesroles, reporting structure, and independenceof the audit team.
* Example:TheIS audit team's roleinrisk assessmentsis outlined in the charter.
* Annual Audit Plan (Incorrect - B)
* Outlinesaudit activitiesbutdoes not define roles and responsibilities.
* Engagement Letter (Incorrect - C)
* Used forspecific audits, not theentire audit function.
* Audit Scope Letter (Incorrect - D)
* Detailswhat is coveredin an audit but doesnot define responsibilities.
References:
* ISACA CISA Review Manual
* COBIT 2019 (Audit Governance)

NEW QUESTION: 511
□□□ □□ □□ □□□□□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □ □□□□?
A. □□□□□□□ □□ 2□□ □□□□□□ □□□□□.
B. □□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□.
C. □□ □□ □□□ □□ □□ □□ □□□ □□□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
The effectiveness of an organization's security awareness program can be measured by capturing data on changes in the way people react to threats, such as the ability to recognize and avoid social engineering attacks1. An increase in the number of phishing emails reported by employees indicates that they are more aware of the signs and risks of phishing, and are more likely to take appropriate actions to prevent or mitigate the impact of such attacks23.
References
1: The Importance Of Measuring Security Awareness 2: Measuring the effectiveness of your security awareness program 3: How effective is security awareness training?

NEW QUESTION: 512

□□□ □□ □ □□□ □□ □□□□□ □□□□ IS □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?

A. □□□ □□□□ □□□□ □□□□ □□□□ □□□□.

B. □□ □□ □ □□ □□□ □□□□□ □□□□□.

C. □□ □□ □□□□ □□ □ □□ □□□□ □□□ □□□□□.

D. □□□□ □□ □□ □□□□□□(CMDB)□ □□□□.

Answer: (SHOW ANSWER)

The greatest concern to an IS auditor who is assessing an organization's configuration and release management process is that changes and change approvals are not documented. This is because documentation is essential for ensuring the traceability, accountability, and quality of the changes made to the configuration items (CIs) and the releases deployed to the production environment. Without documentation, it would be difficult to verify the authenticity, validity, and authorization of the changes, as well as to identify and resolve any issues or incidents that may arise from the changes. Documentation also helps to maintain compliance with internal and external standards and regulations, as well as to facilitate audits and reviews.

The other options are not as concerning as option B, although they may also indicate some weaknesses in the configuration and release management process. The organization does not use an industry-recognized methodology, but this does not necessarily mean that their process is ineffective or inefficient. The organization may have developed their own methodology that suits their specific needs and context. However, using an industry-recognized methodology could help them adopt best practices and improve their process maturity. All changes require middle and senior management approval, but this may not be a problem if the organization has a clear and streamlined approval process that does not cause delays or bottlenecks in the change implementation. However, requiring too many approvals could also introduce unnecessary complexity and bureaucracy in the process. There is no centralized configuration management database (CMDB), but this does not mean that the organization does not have a way of managing their CIs and their relationships. The organization may use other tools or methods to store and access their configuration data, such as spreadsheets, documents, or repositories. However, having a centralized CMDB could help them improve their visibility, accuracy, and consistency of their configuration data.

References:

* 1: The Essential Guide to Release Management | Smartsheet
* 2: 5 steps to a successful release management process - Lucidchart
* 3: Configuration Management process overview - Micro Focus
* 4: Release and Deployment Management process overview - Micro Focus

NEW QUESTION: 513

□□ □ □□ □□□ □□□ □□ IT □□ □□□□ □□□ □□ IT □□ □□□□ □□□□ □□ □□ □□□□□ □□□□ □□ □□□ □□□□□□. □□ □ IS □□□□ □□ □□ □□ □□□ □□□□□?

A. □□ IT □□□□□□ □□□□.

B. IT □□□□ □□□□□ □□□□□.

C. IT □□□□□□ □□ □□□ □□□□□□□.

D. □□ □□ □□□ □□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 514

IS □□□□ □□□ IT □□□ □□□□□ □□ □□□ □□□ □□ □ □□□□ □□□ □ □ □□□□□□. □□□□ □□ □□□ □□ □□ □□ □□ □□□ □□ □ □□□□□?

A. □□□□□ □□ □□□ □□□ □□□.

B. □□□□□ □□ □□□□ □□ □□□ □□□□□ □□□.

C. □□□□□ □□ □□□□ □□□ □□□□ □□□□□ □□□.

D. □□ □□□ □□ □□□ □□□ □□□□ □□ □□□□□ □□□.

Answer: D (LEAVE A REPLY)

Low-priority jobs typically involve non-critical processes or tasks that do not immediately impact business operations. The best approach to handling such jobs is to schedule them subject to resource availability. This ensures that high-priority tasks can access resources when needed without being affected by the execution of low-priority tasks.

* Avoiding Low-Priority Jobs (Option A)is not feasible because even low-priority tasks may be necessary for maintenance or support activities.
* Including Major Functions in Low-Priority Jobs (Option B)contradicts the classification of "low- priority" because major functions are usually critical.
* Allocating Optimal Resources to Low-Priority Jobs (Option C)is inefficient as resources should primarily be allocated to high-priority tasks.

Scheduling based on resource availability optimizes the use of resources, avoids unnecessary delays in high- priority activities, and ensures that low-priority tasks are executed without disrupting overall operations. This aligns with best practices in IT resource management and scheduling.

Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 515

IS □□□□ □□ □□□ □□□□□□ □□□□ □□ □□ □□□ □□□ □□□□ □□□ □.

A. □□ □□ □□.

B. □□□□ □□ □□ □□.

C. □□□□ □□□□□.

D. □□ □□□ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Awalk-through of job functionsprovides direct evidence thatseparation of duties (SoD)is implemented effectively. It involves observing employees as they perform tasks to confirm that no single person has excessive privileges.
* Walk-through of Job Functions (Correct Answer - D)
* Confirms that duties are appropriately divided in real-world operations.
* Helps verify whether security policies and controls are enforced.
* Example:An auditor observes that the same person cannot create and approve financial transactions.
* Review of Personnel Files (Incorrect - A)
* Personnel files contain job details but do not confirm how duties are performed.
* Analysis of Documented Job Descriptions (Incorrect - B)
* Job descriptions may be outdated or inaccurate.
* Review of Organizational Chart (Incorrect - C)
* Shows reporting relationships but does not confirm SoD implementation.
References:
* ISACA CISA Review Manual
* COBIT 2019: Risk Management and Governance
* ISO 27001: Segregation of Duties Control

NEW QUESTION: 516
□□ □ IT □□□ □□□ □□□ □□□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□□
B. □□□□□□ □□□□
C. □□□□□□ □□□□(EA)
D. □□ □□ □□(KPI)
Answer: A (LEAVE A REPLY)
The most useful tool for determining whether the goals of IT are aligned with the organization's goals is a balanced scorecard. A balanced scorecard is a strategic management system that translates an organization's vision and mission into a set of objectives and measures across four perspectives: financial, customer, internal process, and learning and growth. A balanced scorecard helps align IT goals with organizational goals by linking them to a common strategy map that shows how IT contributes to value creation and performance improvement in each perspective. A balanced scorecard also helps monitor and evaluate IT performance against predefined targets and indicators. Enterprise dashboard, enterprise architecture (EA), and key performance indicators (KPIs) are not the most useful tools for determining whether the goals of IT are aligned with the organization's goals. These tools may help communicate, design, or measure IT goals or activities, but they do not provide a comprehensive framework for aligning IT goals with organizational goals across multiple dimensions.

NEW QUESTION: 517
IT □□□□ □□ □□ □ □□ □□□□ □ □□□ □□□□□?
A. IT □□□ □□□□□□ □□□□.
B. □□ IT □□□□ □3□□ □□ □□□□□.
C. IT □□ □□□ □□□□ □□□□□.
D. IT□ □ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
IT value analysis has not been completed is a finding from an IT governance review that should be of greatest concern. IT value analysis is a process of measuring and demonstrating the contribution of IT to the organization's goals and objectives. An IS auditor should be concerned about the lack of IT value analysis, as it may indicate that the IT investments and resources are not aligned with the business needs and expectations, or that the IT performance and outcomes are not monitored and evaluated. The other options are less critical findings that may not have a significant impact on the IT governance.
References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.11
* CISA Review Questions, Answers & Explanations Database, Question ID 218

NEW QUESTION: 518
□□ □ □□ □ □□□ □□□□ □□□ □□ □□ □ □□ □□□ □□□ □□ □□□□□ □□ □□□□□?
A. □□□ □□□ □□□ □□□□□□
B. □□□□ □□ □□□□ □□□□□□
C. □□□□ □□ □□□□□□
D. □□□□□ □□□ □□□□□□
Answer: C (LEAVE A REPLY)
An outsourced accounting application has the most inherent risk and should be prioritized during audit planning because it involves external parties, sensitive data, and complex transactions that are susceptible to material misstatement, error, or fraud12. An outsourced accounting application also requires more oversight and monitoring from the internal audit department to ensure compliance with the service level agreement and the organization's policies and standards3.
References
1: Inherent Risk: Definition, Examples, and 3 Types of Audit Risks 2: 3 Types of Audit Risk - Inherent, Control and Detection - Accountinguide 3: IS Audit Basics: The Core of IT Auditing

NEW QUESTION: 519
□□□ □□ □□□□□ □□□ □ □□□ □□□□ □□ □□□ □□□ □□ □ □□□□ □?

A. □□□□ □□ □□ □□ □□
B. □□□□□□ □□ □□ □□ □□
C. □□□ □□□ □□□ □□ □□
D. □□□□□□ □□□□ □□ □□□ □□ □□
Answer: C (LEAVE A REPLY)
The most important responsibility of data owners when implementing a data classification process is determining appropriate user access levels (option C). This is because:
Data owners are the persons or entities that have the authority and responsibility for the business processes and functions that collect, use, store, and dispose of data1.
Data owners are accountable for ensuring that the data is handled in compliance with the applicable laws, regulations, policies, and standards, such as the GDPR and the PIPEDA1234.
Data owners are in the best position to determine the purpose and necessity of collecting and retaining data, as well as the risks and benefits associated with it1.
Data owners should consult with other stakeholders, such as the risk manager, the database administrator (DBA), and the privacy manager, to establish and implement appropriate data classification policies and procedures2.
Data classification is the process of organizing data in groups based on their attributes and characteristics, and then assigning class labels that describe a set of attributes that hold true for the corresponding data sets345.
Data classification helps organizations to identify, manage, protect, and understand their data, as well as to comply with modern data privacy regulations345.
Data classification also helps to determine appropriate user access levels, which means defining who can access, modify, share, or delete data based on their roles, responsibilities, and needs345.
Determining appropriate user access levels is the most important responsibility of data owners when implementing a data classification process, as it ensures that only authorized and legitimate users can access sensitive or important data. This provides confidentiality, integrity, availability, and accountability of data345.
Reviewing emergency changes to data (option A), authorizing application code changes (option B), and implementing access rules over database tables (option D) are not the most important responsibilities of data owners when implementing a data classification process. These are more related to the operational aspects of data management, which are usually delegated to other roles, such as the DBA or the IT staff. The data owner should oversee and approve these activities, but not perform them directly1.

NEW QUESTION: 520
□□ □□□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□ □ □□ □□□□ □□ □□ □ □□□□□?
A. □□□□ □□□□ □□□□
B. □□□ □□□□ □□□ □□

C. □□ □□ □□ □□
D. □□□ □□ □□
Answer: A (LEAVE A REPLY)
The most effective method for detecting the presence of an unauthorized wireless access point on an internal network is A. Continuous network monitoring. This is because continuous network monitoring can capture and analyze all the wireless traffic in the network and identify any rogue or spoofed devices that may be connected to the network without authorization. Continuous network monitoring can also alert the system administrator of any suspicious or anomalous activities on the network and help to locate and remove the unauthorized wireless access point quickly.
Periodic network vulnerability assessments (B) can also help to detect unauthorized wireless access points, but they are not as effective as continuous network monitoring, because they are performed at fixed intervals and may miss some devices that are added or removed between the assessments. Review of electronic access logs can provide some information about the devices that access the network, but they may not be able to detect devices that use fake or stolen credentials or devices that do not generate any logs.
Physical security reviews (D) can help to prevent unauthorized physical access to the network ports or devices, but they may not be able to detect wireless access points that are hidden or disguised as legitimate devices.

NEW QUESTION: 521
IT □□□□□□ □□ □□□(ROI) □□□□ □ □□ □□□ □□□ □□□□.
A. □□□□ □□ □□.
B. □□ □□ □□.
C. □□ □□ □□.
D. □□ □□□ □□□□ □□.
Answer: D (LEAVE A REPLY)
One benefit of return on investment (ROI) analysis in IT decision making is that it provides the basis for allocating financial resources. ROI analysis is a method of evaluating the profitability or cost-effectiveness of an IT project or investment by comparing the expected benefits with the required costs. ROI analysis can help IT decision makers prioritize and justify their IT initiatives, allocate their financial resources optimally, and demonstrate the value contribution of IT to the organization's goals and objectives. Basis for allocating indirect costs, cost of replacing equipment, and estimated cost of ownership are not benefits of ROI analysis in IT decision making. These are more inputs or outputs of ROI analysis that could be used to calculate or estimate the costs or benefits of an IT project or investment. References: [ISACA CISA Review Manual 27th Edition], page 307

NEW QUESTION: 522

□□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□□□□. □□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□□ □□□□□□□. IS □□□□ □□ □□□□ □□□ □□□□.

A. □□ □□□ □□□ □□ □□ □□□ □□□ □ □□□□.

B. □□ □ □□ □□ □□ □□□ □□ □□□□ □□ □□ □□□ □□□□ □□□□.

C. □□□ □□ □□ □ □□□ □□ □□□□□□□.

D. □□ □□□ □□ □□ □□□□□ □□□□□□□.

Answer: A (LEAVE A REPLY)

An IS auditor's primary concern would be whether the recovery site devices can handle the storage requirements. The storage requirements are determined by the amount and type of data that needs to be backed up and restored in case of a disaster at the primary data center. The recovery site devices should have enough capacity, performance, reliability, and compatibility to meet these requirements.

If the recovery site devices cannot handle the storage requirements, then there is a risk that some data may not be backed up properly or may not be available for recovery when needed. This couldresult in data loss, corruption, or inconsistency, which could affect the business continuity and integrity of the organization.

Therefore, an IS auditor should verify that:

* The recovery site devices have sufficient storage space to accommodate all the data that needs to be backed up from the primary data center.
* The recovery site devices have adequate bandwidth and speed to transfer and access data efficiently and effectively.
* The recovery site devices have appropriate security features and controls to protect data from unauthorized access or modification.
* The recovery site devices are compatible with the primary data center devices in terms of hardware, software, format, and protocol.

References:

* 10: What Is a Disaster Recovery Site? Hot, Cold & Warm Site
* 11: Disaster recovery site - What is the ideal distance to mitigate risks? - Advisera
* 12: Offsite Data Backup Storage vs Disaster Recovery (DR) - LINBIT

NEW QUESTION: 523

IS □□□□ □□ □□□ □□ □□ □□(SDLC) □□ □ □□ □□□□ □□□ □□□ □□ □ □□□□□□ □□□ □□□ □□□□□?

A. □□

B. □□

C. □□ □□□

D. □□□

Answer: (SHOW ANSWER)

The design phase of the system development life cycle (SDLC) is where an IS auditor would expect to find that controlshave been incorporated into system specifications,

because this is where the system requirements are translated intodetailed design specifications that include the technical, functional, and security aspects of the system34. The implementation phase iswhere the system is deployed and tested, the development phase is where the system is codedand unit tested, and thefeasibility phase is where the system objectives and scope are defined. References: 3: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.2 4: CISA Online Review Course, Module 4, Lesson 2

NEW QUESTION: 524

IS □□□□ □□□ □□ □□, □□□□□ □ □□□□ □□□□□ □□□ □□□□□. □ □ □ □□ □□□□□□ □□□□(EA) □□□ □ □□□ □□ □□□□□? (CISA □□ - □ □ □□□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□□)

A. □□ □□□□

B. □□□ □□□□

C. □□ □□ □□□□

D. □□□□□□ □□□□

Answer: C (LEAVE A REPLY)

The lack of system documentation should be of most concern to an IS auditor reviewing the information systems acquisition, development, and implementation process. This is because system documentation is a vital source of information that describes the system's purpose, functionality, design, architecture, testing, deployment, operation, and maintenance. System documentation helps the IS auditor to understand and evaluate the system's quality, performance, security, compliance, and alignment with the business requirements and objectives. Without system documentation, the IS auditor may not be able to perform a thorough and effective audit of the system, as well as identify any issues or risks that may affect the system's reliability or integrity12.

Data owners are not trained on the use of data conversion tools is not the most concerning issue, although it may indicate a lack of user readiness or competence for the system implementation. Data conversion tools are software applications that help users to transform data from one format or structure to another, such as from legacy systems to new systems. Data owners are users who have the responsibility and authority to manage and control the data within their domain. Data owners should be trained on how to use data conversion tools to ensure that the data is accurately and securely transferred to the new system, as well as to avoid any data loss, corruption, or inconsistency. However, data owners are not the only users who need training for the system implementation, and data conversion tools are not the only tools that need training34.

A post-implementation lessons-learned exercise was not conducted is not the most concerning issue, although it may indicate a lack of continuous improvement or learning culture for the system development and implementation process. A post-implementation lessons-learned exercise is a meeting or a session that takes place after the completion of a system implementation project, where the project team and stakeholders discuss and document the successes and failures of the project, as well as identify any best practices

or areas for improvement for future projects. A post-implementation lessons-learned exercise can help to enhance the project management skills, knowledge, and performance of the project team and stakeholders, as well as to avoid repeating the same mistakes or problems in future projects56.
System deployment is routinely performed by contractors is not the most concerning issue, although it may pose some challenges or risks for the system implementation process. System deployment is the final stage of the system development life cycle (SDLC), where the system is installed and configured on the target environment and made available for use by end-users. System deployment can be performed by internal staff or external contractors, depending on the availability, expertise, and cost of resources. System deployment by contractors may offer some benefits such as faster delivery, lower cost, or higher quality than internal staff. However, system deployment by contractors may also introduce some risks such as loss of control, dependency, or security breaches over the system implementation process

NEW QUESTION: 525
□□ □ □□□ □□□□ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□
B. □□ □□ □□ □□
C. □□□ □□ □□
D. □□ □□ □□
Answer: C (LEAVE A REPLY)
The best source ofinformation for examining the classification of new data is the risk assessment results, because they provide an objective and consistent basis for determining the value, sensitivity, and criticality of the data, as well as the potential impact of unauthorized disclosure, modification, or loss of the data12. The risk assessment results can help to definethe appropriate classification levels and criteria for the data, such as public, internal, confidential, or restricted12. Input by data custodians, security policy requirements, and current levelof protection are not the best sources of information for examining the classification of new data, because they may not reflect the actual risk exposure or business needs of the data. References: 1: CISA Review Manual (Digital Version), Chapter 5, Section5.4.2 2: CISA Online Review Course, Module 5, Lesson 4

NEW QUESTION: 526
□□ □□ □□(DRP) □□□□ □□□□□□□ □□□□ □□ □□ □□□ □□ □ □□□ □□?
A. □□ □□□ □□□ □□□ □□□□□□ □□□□□.
B. □□ □□□ □□□□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□□□.
D. □□□□□ □□ □□□ □□□□□□.

Answer: (SHOW ANSWER)
The best way to determine whether a test of a disaster recovery plan (DRP) was successful is to analyze whether predetermined test objectives were met. Test objectives are specific, measurable, achievable, relevant, and time-bound (SMART) goals that define what the test aims to accomplish and how it will be evaluated. Test objectives should be aligned with the DRP objectives and scope, and should cover aspects such as recovery time objectives (RTOs), recovery point objectives (RPOs), critical business functions, roles and responsibilities, communication channels, backup systems, and contingency procedures. By comparing the actual test results with the expected test objectives, the IS auditor can measure the effectiveness and efficiency of the DRP and identify any gaps or weaknesses that need to be addressed.

NEW QUESTION: 527
□□ □ □□□□ □□□(IM) □□□□□□□ □□ □□ □□□□□ □□□ □□□□ □□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□ □□□
B. □□ □□ □□□□(FTP)
C. □□□□ □□□ □□
D. □□□□□□ □□ □□□
Answer: D (LEAVE A REPLY)
Application level firewalls are the best control to prevent the transfer of files to external parties through instant messaging (IM) applications, because they can inspect and filter network traffic based on application- specific protocols and commands, such as IM file transfer commands. Application level firewalls can block or allow IM file transfers based on predefined rules or policies. File level encryption, file transfer protocol (FTP), and instant messaging policy are not effective controls to prevent IM file transfers, because they do not restrict or monitor IM network traffic. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4.1

NEW QUESTION: 528
IS □□□□ □□ □□ □□□ □□□□ □□ □□ □ □□ □□ □□□□□ □□□?
A. □□ □□□ □□□ □□□ □□ □□ □□□ □□□
B. □□ □□□□ □□ □□□□ □□□ □□□ □□ □□

C. □□ □□□□ □□□ □□ □□□ □□□□ □□ □

D. □□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□

Answer: B (LEAVE A REPLY)

This must be in place before an IS auditor initiates audit follow-up activities, because it indicates that management has acknowledged and accepted the audit findings and recommendations, and has agreed to take corrective actions within a specified timeframe. Audit follow-up activities are the processes and procedures that the IS auditor performs to verify that management has implemented the agreed-upon actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.

The other options are not required to be in place before an IS auditor initiates audit follow-up activities:

* Available resources for the activities included in the action plan. This is a factor that may affect the feasibility and success of the action plan, but it is not a prerequisite for the audit follow-up activities.

The IS auditor should assess the availability and adequacy of the resources for the action plan during the audit planning and execution phases, and provide recommendations accordingly. However, the IS auditor does not need to wait for the resources to be available before initiating the audit follow-up activities.

* A heat map with the gaps and recommendations displayed in terms of risk. This is a tool that may help the IS auditor prioritize and communicate the gaps and recommendations, but it is not a requirement for the audit follow-up activities. A heat map is a graphical representation of data that uses colors to indicate the level of risk or impact of each gap or recommendation. The IS auditor may use a heat map to support the audit report or presentation, but it does not replace the need for a management response with a committed implementation date.

* Supporting evidence for the gaps and recommendations mentioned in the audit report. This is a component that should be included in the audit report, but it is not a condition for the audit follow-up activities. Supporting evidence is the information or data that supports or substantiates the audit findings and recommendations. The IS auditor should collect and document sufficient, reliable, relevant, and useful evidence during the audit execution phase, and present it in the audit report.

However, the IS auditor does not need to have supporting evidence in place before initiating the audit follow-up activities.

NEW QUESTION: 529

IS □□□□ □□ □□ □□ □□□ □□□□□ □□□□ □□ □□□ □□□ □, □□ □□ □□ □ □□ □ □□□□ □□□ □□ □□□□□?

A. □□□ □□ □□□ □□ □□□□□□□.

B. □□□□□□□ □□□□ □□□□□□□.

C. □□□ □□□ □□ □□□ □□□ □□ □□□□ □□□□□.

D. □□□□ □□ □□□□□□ □□□ □□□□□□ □□□□□□□.

Answer: D (LEAVE A REPLY)
Antivirus software has been implemented on the guest operating system only is the observation that an IS auditor would consider the greatest risk when conducting an audit of a virtual server farm for potential software vulnerabilities. A virtual server farm is a collection of servers that run multiple virtual machines (VMs) on a single physical host using a software layer called a hypervisor. A guest operating system is the operating system installed on each VM. Antivirus software is a software program that detects and removes malicious software from a computer system. If antivirus software has been implemented on the guest operating system only, it means that the hypervisor and the host operating system are not protected from malware attacks, which could compromise the security and availability of all VMs running on the same host.
Therefore, antivirus software should be implemented on both the guest and host operating systems as well as on the hypervisor. References: CISA Review Manual, 27th Edition, page 378

NEW QUESTION: 530
□□□ □□□□ □□□ □□(BCP)□ □□□ □ IS □□□□ □□ □□□□ □□□ □□ □ □□□□□?
A. □□ □□□ □□□□ □ □□□□□□ □□□□ □□□□ □□ □□□□.
B. □□ □□□ □□□ □□ □□ □□(RPO)□□ □□□.
C. □□ □□□ □□ □□□ □□ □□ □□(RTO)□□ □□□.
D. □□ □□ □□(RPO)□ □□ □□ □□(R TO)□ □□□□ □□□□.
Answer: (SHOW ANSWER)
A business continuity plan (BCP) is a document that outlines how an organization will continue its critical functions in the event of a disruption or disaster. A BCP should include the following elements1:
Business impact analysis: This is the process of identifying and prioritizing the key business processes and assets that are essential for the organization's survival and recovery.
Risk assessment: This is the process of identifying and evaluating the potential threats and vulnerabilities that could affect the organization's business continuity.
Recovery strategies: These are the actions and procedures that the organization will implement to restore its normal operations as quickly and effectively as possible after a disruption or disaster.
Recovery objectives: These are the metrics that define the acceptable level of recovery for the organization's business processes and assets. The two main recovery objectives are:
Recovery point objective (RPO): This is the maximum amount of data loss that the organization can tolerate in terms of time. For example, an RPO of one hour means that the organization can afford to lose up to one hour's worth of data after a disruption or disaster.

Recovery time objective (RTO): This is the maximum amount of time that the organization can tolerate to restore its normal operations after a disruption or disaster. For example, an RTO of four hours means that the organization must resume its normal operations within four hours after a disruption or disaster.
Testing and validation: This is the process of verifying and evaluating the effectiveness and efficiency of the BCP and its components. Testing and validation can include various methods, such as:
Tabletop exercises: These are discussion-based sessions where team members meet in an informal setting to review and discuss their roles and responsibilities during a disruption or disaster scenario. A facilitator guides participants through a discussion of one or more scenarios2.
Simulation exercises: These are more realistic and interactive sessions where team members perform their roles and responsibilities during a simulated disruption or disaster scenario. A facilitator controls and monitors the simulation and injects events and challenges3.
Full-scale exercises: These are the most complex and realistic sessions where team members perform their roles and responsibilities during a real-life disruption or disaster scenario. A facilitator coordinates and evaluates the exercise with external stakeholders, such as emergency services, media, or customers4.
As an IS auditor, your greatest concern when reviewing the organization's BCP would be
A. The recovery plan does not contain the process and application dependencies.

NEW QUESTION: 531
□□ □ □□ □□□ □□□□ □□ □□□□□□ □□□□ □□ □□ □ □□□ □ □□□ □?
A. □□□□ □□ □□□□□□ □□□□□□ □□□ □□□□□ □□□□ □□□□.
B. □□□□ □□□ □□ □□□□□□ □□□□ □ □□□□.
C. □□ □□□ □□□ □□□ □□□□ □□ □□□□□□ □□□□□.
D. □□□□ □□ □□ □□□ □□□□□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)
Unauthorized changes can be moved into production is the best concern that is addressed by securing production source libraries. Production source libraries contain the source code of programs that are used in the production environment. Securing production source libraries means implementing access controls, change management procedures, and audit trails to prevent unauthorized or improper changes to the source code that could affect the functionality, performance, or security of the production programs. The other options are less relevant concerns that may not be directly addressed by securing production source libraries, but rather by other controls such as program approval, version control, or change testing. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3.21
* CISA Review Questions, Answers & Explanations Database, Question ID 213

NEW QUESTION: 532
IS □□□□ □□□□□ □□□□□ □□□□ □□□□ □□□□. □ □□□ □□ □□ □ □□ □□□ □□ □□ □□ □ □□ □ □□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□
B. □□□ □□□□ □□□ □□□ □ □□
C. □□ □□□ □□ □□
D. □□ □□□ □□□□
Answer: D (LEAVE A REPLY)
The greatest concern for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger is the inaccuracy of financial reporting. A subledger is a detailed record of transactions for a specific account, such as accounts receivable, accounts payable, inventory, or fixed assets.
A main ledger is a summary record of all transactions for all accounts in an accounting system. The mapping of accounts between a subledger and a main ledger is the process of linking or reconciling the transactions in the subledger with the corresponding entries in the main ledger. If there are flaws in the mapping of accounts, such as missing, duplicated, or incorrect transactions, the main ledger may not reflect the true financial position and performance of the organization. This may lead to inaccurate financial reporting, which may affect decision making, compliance, auditing, taxation, and stakeholder confidence.
Double-posting of a single journal entry, inability to support new business transactions, and unauthorized alteration of account attributes are not the greatest concerns for an IS auditor if there are flaws in the mapping of accounts between a front-end subledger and a main ledger. These are possible consequences or causes of flaws in the mapping of accounts, but they do not have as significant an impact as inaccuracy of financial reporting. Double-posting of a single journal entry may result in errors or discrepancies in the main ledger balances. Inability to support new business transactions may indicate limitations or inefficiencies in the accounting system design or configuration. Unauthorized alteration of account attributes may suggest weaknesses or breaches in access control or segregation of duties.

NEW QUESTION: 533
□□ □ □□□ □□ □□□ □□□□ □□ □□□ □□□(EUC) □□□□□□□ □□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. EUC □□
B. EUC □□□ □□
C. EUC □□ □□ □□□□
D. EUC □□ □□□ □□□
Answer: A (LEAVE A REPLY)
The best way to improve the visibility of end-user computing (EUC) applications that support regulatory reporting is to maintain an EUC inventory, as this provides a

comprehensive and up-to-date list of all EUC applications, their owners, their locations, their purposes, and their dependencies. An EUC inventory can help identify and manage the risks associated with EUC applications, such as data quality, security, compliance, and continuity. EUC availability controls, EUC access control matrix, and EUC tests of operational effectiveness are important for ensuring the reliability and security of EUC applications, but they do not improve the visibility of EUC applications as much as an EUC inventory. References: CISA Review Manual (Digital Version), Chapter 3: Information Systems Acquisition, Development and Implementation, Section
3.4: End-user Computing

NEW QUESTION: 534
□□□ □□□□ □□ IS □□□□□ □□ □□□□ □□ □□□ □□□ □□ □□□ □□ □□□ □□□□□. □□ □ □□ □□ □□□ □□□ □□□□ □ □□ □□□□□□?
A. □□□□□ □□ □□ □□
B. □□□□ □□□□□ □□□□
C. □□□ □□□□□ □□ □□□ □□ □□
D. □□ □□ □□ □□ □□
Answer: A (LEAVE A REPLY)
The most effective way to detect an intrusion attempt is to periodically review log files, which record the activities and events on a system or network. Log files can provide evidence of unauthorized access attempts, malicious activities, or system errors. Configuring the router as a firewall, using smart cards with one-time passwords, and installing biometrics-based authentication are preventive controls that can reduce the likelihood of an intrusion, but they do not detect it. References: ISACA CISA Review Manual 27th Edition, page 301

NEW QUESTION: 535
□□ □□ □ □□ □□□ □□ IS □□□□ □□ □□ □□(CSA)□ □□□□ □□□□ □ □□ □□□□ □□□ □ □□□□?
A. □□ □□ □□
B. CSA □□ □□
C. □□ □□ □□
D. CSA □□□ □□
Answer: D (LEAVE A REPLY)
Developing the CSA questionnaire is an activity that would allow an IS auditor to maintain independence while facilitating a control self-assessment (CSA). An IS auditor can design and provide a CSA questionnaire to help the business units or process owners to evaluate their own controls and identify any issues or improvement opportunities. This will enable an IS auditor to support and guide the CSA process without compromising their objectivity or independence. The other options are activities that would impair an IS auditor's

independence while facilitating a CSA, as they involve implementing, completing, or developing remediation actions for control issues. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.41
* CISA Review Questions, Answers & Explanations Database, Question ID 215

NEW QUESTION: 536
□□□□□ □□□□ □□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □ □□□.
A. □□ □□□ □□□ □□□ □□□ □□□ □□□□□.
B. IS □□□□ □□□□□□ □□□□□□.
C. IS □□□□ □□ □□(QA) □□ □□□□□□.
D. □□ □□□ □□□□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best way to provide assurance that a project is adhering to the project plan is to conduct compliance audits at major system milestones. A compliance audit is a systematic and independent examination of the project's activities, documents, and deliverables to determine whether they conform to the project plan and its specifications, standards, and requirements1. A major system milestone is a significant point or event in the project's life cycle that marks the completion of a phase, stage, or deliverable2.
By conducting compliance audits at major system milestones, the auditor can provide assurance that the project is adhering to the project plan by:
Verifying that the project's scope, schedule, budget, quality, and risks are aligned with the project plan and its objectives1 Identifying any deviations, discrepancies, or non-compliances that may affect the project's performance or outcome1 Recommending and monitoring corrective and preventive actions to address the identified issues and improve the project's compliance1 Reporting and communicating the audit findings, conclusions, and recommendations to the relevant stakeholders1 The other options are not as effective as conducting compliance audits at major system milestones for providing assurance that the project is adhering to the project plan. Requiring design reviews at appropriate points in the life cycle is a useful technique for ensuring that the project's design meets the user and business requirements and follows the design standards and best practices3. However, design reviews are not sufficient for providing assurance that the project is adhering to the project plan, as they do not cover other aspects of the project such as schedule, budget, quality, or risks. Having an IS auditor participate on the steering committee is a possible way for providing assurance that the project is adhering to the project plan, as the auditor can provide independent advice and oversight to the steering committee on quality management issues and remediation efforts4. However, this may not be feasible or appropriate for every project, as it may create a conflict of interest or compromise the auditor's objectivity and independence. Having an IS auditor participate on the quality assurance (QA) team is another possible way for providing assurance that the project is adhering to the project plan, as the auditor can assist the QA team in implementing

procedures to facilitate adoption of quality management best practices5. However, this may also not be feasible or appropriate for every project, as it may create a conflict of interest or compromise the auditor's objectivity and independence.
Therefore, option D is the correct answer.
References:
What Is Compliance Audit? Definition & Process | ASQ
What Is A Project Milestone? - The Basics
Design Review - an overview | ScienceDirect Topics
Project success through project assurance - Project Management Institute Quality Assurance Team: Roles & Responsibilities

NEW QUESTION: 537
□□ □ □□ □□□□ □□□(RPA) □□□□□ □□□□□□□ □□□□□ □□ □□□□ □□ □□□ □□□□□?
A. IT □□
B. □□□
C. □□□□□□□
D. □□□ □□□
Answer: (SHOW ANSWER)
The business owner is best positioned to catalog and inventory robotic process automation (RPA) processes because they understand the processes, objectives, and associated risks. They ensure that RPA aligns with business goals and compliance requirements.
* IT Personnel (Option A):Typically support implementation and maintenance but may lack insight into business processes.
* Information Security Personnel (Option C):Focus on securing processes but are not responsible for inventorying them.
* Data Steward (Option D):Primarily responsible for data governance, not RPA process inventory.
Reference:ISACA CISA Review Manual, Job Practice Area 1: Governance and Management of IT.

NEW QUESTION: 538
IS □□□□ □□□ □□□□□□ □□ □□□ □□ □□□ □□□ □□□□ □ □□ □ □ □ □□□□□□. □□ □ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□ □□□□ □?
A. □□□ □□□
B. □□□ □□□
C. □□□ □□□
D. □□□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 539
IS □□□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□□ □□□□. IS □□□□ □ □ □ □□ □□□ □□ □□□□ □□□?
A. □□ □□□□ □□□□□.
B. □□□ □□□□□□.
C. □□ □□ □□□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
An audit universe is a comprehensive list of all the auditable entities, processes, and activities within an organization. It helps the IS auditor to identify the scope, objectives, and priorities of the audit plan, as well as the resources and methodologies required to conduct the audits. An audit universe can also help the IS auditor to ensure that all the key risks, controls, and regulations are covered by the audit plan, and that there are no gaps or overlaps in the audit coverage.
The first activity that the IS auditor should perform when preparing a plan for audits to be carried out over a specified period is to determine the audit universe. This involves defining the criteria and methods for identifying and categorizing the auditable units, such as by business function, process, system, location, or risk level. The IS auditor should also consult with the management and other stakeholders to obtain their input and expectations for the audit plan. The IS auditor should then document and validate the audit universe, and update it regularly to reflect any changes in the organization's structure, operations, or environment.
The other three activities are also important for preparing an audit plan, but they should be performed after determining the audit universe. Allocating audit resources involves assigning staff, time, budget, and tools to each audit based on their complexity, priority, and availability. Prioritizing risks involves assessing the likelihood and impact of each risk associated with each auditable unit, and ranking them according to their significance and urgency. Reviewing prior audit reports involves analyzing the findings, recommendations, and actions from previous audits related to each auditable unit, and evaluating their current status and relevance.
Therefore, determining the audit universe is the best answer.
References:
* Audit Universe - UPDATED 2022 - Examples, Templates & More!
* 01 February 2023 Audit universe - IIA

NEW QUESTION: 540
IS □□□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□ □□ □□ □(ICS)□ □□□□ □□□□. □□□□ □□□ □□ □□□ □□ □□□□ □□□□ □□ □?
A. □□□ □□ □□□□ □□ □□□ □□□□ □□□□.
B. □□□ □□□ □□□ □ □□□.

C. □□ □□ □□(DRP)□ □□□□ □□ □□□□.
D. □□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The most significant concern for an IS auditor when reviewing an industrial control system (ICS) that uses older unsupported technology in the scope of an upcoming audit is that there is a greater risk of system exploitation. System exploitation is an attack that occurs when an unauthorized entity or individual takes advantage of a vulnerability or weakness in a system to compromise its security or functionality. System exploitation can cause harm or damage to the system or its users, such as data loss, corruption, theft, manipulation, denial of service (DoS), etc. An ICS that uses older unsupported technology poses a high risk of system exploitation, as older technology may have known or unknown vulnerabilities or defects that have not been patched or fixed by the vendor or manufacturer, and unsupported technology may not receive any updates or support from the vendor or manufacturer in case of issues or incidents. Attack vectors are evolving for industrial control systems is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Attack vectors are methods or pathways that attackers use to gain access to or attack a system. Attack vectors are evolving for industrial control systems, as attackers are developing new techniques or tools to target ICSs that are increasingly connected and complex. However, this concern may not be specific to older unsupported technology, as it may affect any ICS regardless of its technology level. Disaster recovery plans (DRPs) are not in place is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. DRPs are documents that outline the technical and operational steps for restoring the IT systems and infrastructure that support critical functions or processes in the event of a disruption or disaster. DRPs are not in place, as they may affect the availability and continuity of the ICS and its functions or processes in case of a failure or incident. However, this concern may not be related to older unsupported technology, as it may apply to any ICS regardless of its technology level.
Technical specifications are not documented is a possible concern for an IS auditor when reviewing an ICS that uses older unsupported technology in the scope of an upcoming audit, but it is not the most significant one. Technical specifications are documents that describe the technical characteristics or requirements of a system or component, such as functionality, performance, design, etc. Technical specifications are not documented, as they may affect the understanding, maintenance, and improvement of the ICS and its components. However, this concern may not beassociated with older unsupported technology, as it may affect any ICS regardless of its technology level.

NEW QUESTION: 541
□□ □ IT □□□□ □□□□□ □□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□ □□ □□□□□

B. □□ □□□
C. □□ □□(QA) □□
D. □□ □□ □□
Answer: (SHOW ANSWER)
The best source of information for assessing the effectiveness of IT process monitoring is performance data.
Performance data is a type of information that measures and reports on the results or outcomes of IT processes, such as availability, reliability, throughput, response time, or error rate. Performance data can help assess the effectiveness of IT process monitoring by providing quantitative and qualitative indicators of whether IT processes are meeting their objectives, standards, or expectations. The other options are not as good as performance data in assessing the effectiveness of IT process monitoring, as they do not provide direct or objective evidence of IT process results or outcomes. Real-time audit software is a type of tool that can help automate and facilitate audit activities, such as data collection, analysis, or reporting, but it does not provide information on IT process performance. Quality assurance (QA) reviews are a type of activity that can help evaluate and improve the quality of IT processes, products, or services, but they do not provide information on IT process performance. Participative management techniques are a type of method that can help involve and motivate IT staff in decision-making and problem-solving processes, but they do not provide information on IT process performance. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 542
□□□ □□ □□ □□(DRP)□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □ □□□□?
A. DRP□ □□ □□ □□□□ □□ □□□ □□ □□□□□.
B. DRP□ □□ □□□□□ □□□□ □□□□□.
C. IT □□□ □□□□□ □□ DRP□ □□□□□□ □□□□□.
D. DRP□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
The greatest concern for an IS auditor reviewing an organization's disaster recovery plan (DRP) is that the DRP has not been updated since an IT infrastructure upgrade. This could render the DRP obsolete or ineffective, as it may not reflect the current configuration,

dependencies or recovery requirements of the IT systems. The IS auditor should ensure that the DRP is reviewed and updated regularly to align with any changes in the IT environment. The DRP has not been formally approved by senior management is a concern for an IS auditor reviewing an organization's DRP, but it is not as critical as ensuring that the DRP is up to date and valid. The DRP has not been distributed to end users or the DRP contains recovery procedures for critical servers only are issues that relate to the communication or scope of the DRP, but not to its validity or effectiveness. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 389

NEW QUESTION: 543
□□□□ □□□□ □□ □ 80□ □□ □□□ □□□□ □□□ □□□ □□□□□ □□□.
IS □□□□ □□□ □□□□ □□□?
A. □□□□□□□ □□□□□.
B. □□ □□□ □□(ITF)□ □□□□□.
C. □□□□ □□ □□□□□□ □□□□□.
D. □□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
Generalized audit software is a type of computer-assisted audit technique (CAAT) that allows the IS auditor to perform various audit tasks on the data stored in different file formats and databases1. Generalized audit software can help the IS auditor to select a sample for testing that includes the 80 largest client balances and a random sample of the rest, by using functions such as sorting, filtering, stratifying, and randomizing the data23. Generalized audit software can also help the IS auditor to perform other audit procedures on the sample, such as verifying the accuracy, completeness, and validity of the data4. References
1: Generalized Audit Software (GAS) - ISACA 2: Audit Sampling - ISACA 3: How to use generalized audit software to perform audit sampling 4: Generalized Audit Software: A Review of Five Packages

NEW QUESTION: 544
□□□ □□□ □□ □□ IS □□□□ □ □□□□□□ □□ □□□ □□□□□ □□□□□ □□. □□□□ □□□□ □□□ □□ □□ □□□ □□□□ □□□□ □□ □□□□□□. □□□ □□□ □□□□ □ □□ □□□ □□ □□□?
A. □□ □□□ □□□
B. □□□□ □□□
C. □□□□□□□
D. □□□□ □□□
Answer: (SHOW ANSWER)
The project manager should be accountable for managing the risks to project benefits. Project benefits are the expected outcomes or value that a project delivers to its stakeholders, such as improved efficiency, quality, customer satisfaction, or revenue.

Project risks are uncertain events or conditions that may affect the project objectives, scope, budget, schedule, or quality. The project manager is responsible for identifying, analyzing, prioritizing, responding to, and monitoring project risks throughout the project life cycle. The other options are not accountable for managing project risks, as they have different roles and responsibilities. The enterprise risk manager is responsible foroverseeing the organization's overall risk management framework and strategy, but not for managing specific project risks. The project sponsor is responsible for initiating, approving, and supporting the project, but not for managing project risks. The information security officer is responsible for ensuring that the project complies with the organization's information security policies and standards, but not for managing project risks. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3