ISACA.CISA-KR.v2025-04-03.q628

□□□□:	CISA-KR
□□□□:	Certified Information Systems Auditor (CISA Korean Version)
□□□:	ISACA
□□ □□ □□□:	628
□□:	v2025-04-03
# □□ □:	3154
# □□ □□□:	6280
https://www.krdump.com/ISACA.CISA-KR.v2025-04-03.q628.html	

NEW QUESTION: 1
□□ □□□□ □□□□ □□□ □□□□□□□□ □□□ □□□□ □□□□ □□□□ □ □□ □□□□ □□□□.
□□ □ IS □□□□ □□ □□□□ □□ □□□□□?
A. □□□ □□□ □□□□□ □□□□□ □□□□ □□□□.
B. □□ □□ □ □□□ □□ □□ □□ □□ □□□ □□□□ □□□□□.
C. □□□ □□□ □□ □□□□ □□ □□□□□□ □□□□□.
D. □□ □□□ □□ □□ □□□ □□□□□ □□□□□□□.
Answer: (SHOW ANSWER)
Periodic review of scheduled jobs is crucial to prevent unauthorized or outdated jobs from running, which could lead to security risks, data inconsistencies, or compliance issues.If the inventory of scheduled jobs is not reviewed periodically (A), it could result in jobs running with incorrect parameters, unauthorized transfers, or failure to decommission obsolete processes.
Other options:
Automated support ticket creation (B)is beneficial but is not as critical as ensuring the overall accuracy and security of job execution.
Restricting access to scheduling changes (C)is a security control, but its absence is not the most pressing concern compared to unreviewed jobs.
Notification alerts to a support group (D)is a good practice but does not replace the need for a formal review process.
Reference:ISACA CISA Review Manual, Information Systems Operations and Business Resilience

NEW QUESTION: 2
□□ □□ □□□ □□□ □ IT □□ □□□□ □□ □□ □□□□ □ □□□ □□□□□?
A. IT □□□ □□□ □□□ □□

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

NEW QUESTION: 3
□□□ □□□ □ IS □□□□ □□□ □□ □□□ □□ □3□ □□□□□ □□ □□ □□□ □ □□□□ □□ □□□□□.
A. □□ □ □□□□ □□ □□ □□□ □□□□□.
B. □□□ □□□□ □□□□□ □□ □ □□□ □□□□□.
C. □□□□ □□□ □□□ □□□□ □□□□ □□□□□.
D. □□□□ □□ 12□□ □□□ □□□□□□□.
Answer: A (LEAVE A REPLY)
It is acceptable for an IS auditor to rely on a third-party provider's external audit report on service level management when the scope and methodology meet audit requirements. This means that the external audit report covers the same objectives, criteria, standards and procedures that the IS auditor would use to assess the service level management. This way, the IS auditor can avoid duplication of work and reduce audit costs and efforts. The service provider's certification and accreditation, the report's confirmation of service levels and the report's release date are not sufficient to justify reliance on the external audit report. References: CISA Review Manual (Digital Version) , Chapter 2, Section 2.3.3.

NEW QUESTION: 4
□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□ □□ □ □□ □□□ □□□□ □□?
A. □□□□ □□□
B. □□□□ □□□
C. □□□□ □□□
D. □□□□ □□□
Answer: (SHOW ANSWER)
The best option for ensuring confidentiality through the use of asymmetric encryption is to encrypt a message with the recipient's public key (option A). This is because: Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner12. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key12.

Encrypting a message with the recipient's public key ensures that only the recipient can decrypt it with their private key. This provides confidentiality, which means that the message is protected from unauthorized access or disclosure12.
Encrypting a message with the sender's private key (option B) does not ensure confidentiality, but rather authentication, which means that the message can be verified as coming from the sender. This is because anyone can decrypt the message with the sender's public key, but only the sender can encrypt it with their private key12.
Encrypting a message with the sender's public key (option C) or the recipient's private key (option D) does not make sense, as it would render the message unreadable by both parties. This is because neither party has the corresponding key to decrypt it12.
Therefore, the best option for ensuring confidentiality through the use of asymmetric encryption is to encrypt a message with the recipient's public key (option A), as this ensures that only the recipient can decrypt it with their private key.
References: 1: What is asymmetric encryption? | Asymmetric vs. symmetric ... - Cloudflare 2: What is Asymmetric Encryption? - GeeksforGeeks

NEW QUESTION: 5
IS □□□□ □□□□□□ □□□ □□ □□□ □□ □□□ □□□□ □□□ □□□□□ □ □□□ □□ □□□□□ □□ □□ □□□ □□□□□. □□ □ □ □□□□ □□ □□□ □ □□ □□□□□?
A. □□□□□□ □□ □□
B. □□□ □□□ □□
C. □□□ □□□ □□□
D. □□□ □□□ 1o □□□□
Answer: (SHOW ANSWER)
The most significant risk from not testing patches before putting them into production is the lack of system integrity. Patches are software updates that fix bugs, vulnerabilities or performance issues in an application system. However, patches may also introduce new errors, conflicts or compatibility issues that could affect the functionality, reliability or security of the system4. By not testing patches before putting them into production, the organization exposes itself to the risk of system failures, data corruption or unauthorized access. Loss of application support, outdated system documentation and developer access to production are also risks from not testing patches, but they are not as significant as the lack of system integrity. References:
* CISA Review Manual, 27th Edition, page 2951
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 6
□□ □□□□ □□ □ □□□(PKI)□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □□□?
A. PKI □□□ □□ 1□ □□ □□□□□□ □□□□□.

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

NEW QUESTION: 7
□□ □ IS □□□□ □□□ □□□□ □□□ □ □□ □□□ □□ □□ □□□□□?
A. □□ □□ □□(CSA)
B. □□ □□□ □□
C. □□□□□ □□□
D. □□ □□
Answer: B (LEAVE A REPLY)
The most helpful thing for an IS auditor when assessing the effectiveness of controls is the results of control testing, as this provides objective and reliable evidence of how well the controls are designed and operating in practice. A control self-assessment (CSA) is a technique that involves the participation of process owners and stakeholders in evaluating the effectiveness of controls, but it may not be as rigorous or independent as control testing. Interviews with management are useful for gaining an understanding of the control environment and culture, but they may not reflect the actual performance of controls. A control matrix is a tool that maps the controls to the objectives, risks, and requirements, but it does not measure the effectiveness of controls. References: CISA Review Manual (Digital Version),Chapter 1: Information Systems Auditing Process, Section 1.3: IT Audit Process

NEW QUESTION: 8
IS □□□□ □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□ □□□□ □ □□ □□□□ □□□□ □□□ □□□□□□. □□ □□□□ □□□□□□ □□ □□□□ □□ □ □□□ 6□□□ □□ □□□□ □□□□□. □□ □ □□□□ □□ □□□ □□□□□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□?
A. □□□□□ □□□□ □□□ □□□ □□ □□□ □□□□□□ □□□□□.
B. □□□ □□□□□ □□□□□ □□□□ □□ □□ □□□ □□□□.
C. □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□ □□□□□□□.
D. □□□ □□□□□ □□□□ □□ □□□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. This will limit the exposure of the system to potential attacks and prevent it from compromising other systems on the network. Segregating the system will also reduce the impact of any security incidents that may occur on the system.
Monitoring network traffic attempting to reach the outdated software system (option C) is not the best way to reduce the risk, as it will not prevent or stop any attacks on the system.

It will only provide visibility into the network activity and alert the auditee of any suspicious or malicious traffic.
Verifying all patches have been applied to the software system's outdated version (option A) and closing all unused ports on the outdated software system (option B) are also not the best ways to reduce the risk, as they will not address the underlying issue of using an unsupported version of the software. Patches and ports may still have vulnerabilities that are not fixed by the vendor, and attackers may exploit them to gain access to the system. Therefore, option D is the correct answer.
References:
* Introduction (Part 1 of 7: Mitigating Risks of Unsupported Operating Systems)
* Summary (Part 7 of 7: Mitigating Risks of Unsupported Operating Systems)
* Upgrade, Retire, or Replace Unsupported Software (Part 4 of 7: Mitigating Risks of Unsupported Operating Systems)

NEW QUESTION: 9
□□□□ □□ □□□ □ □□ □□□ □□ □□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□
B. □□□□ □□□□ □ □□ □□□ □□
C. □□□□ □□□□ □□□ □ □□□□□□ □□ □□□□
D. □□□ □□□ □□□□ □□ □□□□
Answer: (SHOW ANSWER)
The most important thing to determine during the planning phase of a cloud-based messaging and collaboration platform acquisition is the types of data that can be uploaded to the platform. This is because different types of data may have different security, privacy, and compliance requirements, depending on the nature, sensitivity, and value of the data. For example, personal data, financial data, health data, or intellectual property data may be subject to various laws and regulations that govern how they can be collected, stored, processed, and shared in the cloud. Therefore, it is essential to identify and classify the types of data that will be uploaded to the platform, and ensure that the platform meets the organization's policies and standards for data protection1.
The other options are not as important as the types of data that can be uploaded to the platform during the planning phase of a cloud-based messaging and collaboration platform acquisition. Option A, role-based access control policies, is a mechanism that defines who can access what data and resources on the platform based on their roles and responsibilities. Role-based access control policies are important for ensuring data security and accountability, but they can be designed and implemented after the platform is acquired2. Option C, processes for on-boarding and off-boarding users to the platform, are procedures that enable or disable user accounts and access rights on the platform. Processes for on-boarding and off-boarding users are important for managing user identities and lifecycles, but they can be developed and executed after the platform is

acquired3. Option D, processes for reviewing administrator activity, are methods that monitor and audit the actions and events performed by administrators on the platform. Processes for reviewing administrator activity are important for detecting and preventing unauthorized or malicious activities, but they can be established and performed after the platform is acquired4.
References:
* Cloud Messaging and Collaboration Services - Maryland.gov DoIT4
* MessageBird acquires real-time notifications and in-app messaging platform Pusher for $35M | TechCrunch2
* Symphony to lead financial market communications with the acquisition of Cloud9 Technologies3
* Cloud messaging and collaboration | Sumo Logic

NEW QUESTION: 10
□□ □ □□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□□□□ □□□ □□□ □□
B. □□□□ □□□□□□ □□□□ □□ □□□□ □□ □□
C. □□ □□□□ □□ □□ □□ □□
D. □□ □□□□ □□ □□ □□□ □□□ □□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 11
IT □□□□□ □□□□ □□ □□□ □□ □□□ □□□ □□□□.
A. □□ □□ □□
B. □□□□ □□□□.
C. □□□ □□□□□□.
D. □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 12

□□□ □□ □□□ □□□□ 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: 13

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

A. □□ □□□ 12□□ □□ □□ □□ □□□□□ □□□□□□.

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

C. □□ □□ □□□□ □□□ □□□ □□□□ □□ □□□□□.

D. □□ □□□ □□□□ □□□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 14

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: 15
□□□□ □□ □□□ □□□ □□□□□□. □□ □ □ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□.
B. □□□ □□ □□□□ □□□□□.
C. □□□ □□ □□□□ □□□□□.
D. □□□□ □□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
The first course of action when a data breach has occurred due to malware is to quarantine the impacted systems. This means isolating the infected systems from the rest of the network and preventing any further communication or data transfer with them. This can help contain the spread of the malware, limit the damage and exposure of sensitive data, and facilitate the investigation and remediation of the incident. Quarantining the impacted systems can also help preserve the evidence and logs that may be needed for forensic analysis or legal action.
References:
* [1] provides a guide on how to respond to a data breach caused by malware and recommends quarantining the impacted systems as the first step.
* [2] explains what is malware and how it can cause data breaches, and suggests quarantining the infected devices as a best practice.
* [3] describes the steps involved in quarantining a system infected by malware and the benefits of doing so.

NEW QUESTION: 16
□□□ □□□□□□ □□□□(EA) □□□ □□ □□□ □□□□□ □□□ □□□□ □□ □□□ □□□□□ □□□□□□. IS □□□□ □ □□□ □□□ □ □□□□ □ □□ □□ □ □□ □□ □ □□□□□?
A. □□□ □□□□ □□□□ □□ □□□□ □□

B. □□□□ □□□□□ □□□ □□□ □□□□ □□□□
C. □□□□ □□□□□ □□□□ □□ □□ □□ □□□ □□
D. □□□ □□□ □□ □□□□□□ □□□ □□
Answer: (SHOW ANSWER)
When reviewing an enterprise architecture (EA) department's decision to change a legacy system's components while maintaining its original functionality, an IS auditor should understand the current business capabilities delivered by the legacy system, as this would help to evaluate whether the change is justified, feasible, and aligned with the business goals and needs. The proposed network topology to be used by the redesigned system, the data flows between the components to be used by the redesigned system, and the database entity relationships within the legacy system are technical details that are less relevant for an IS auditor to understand when reviewing this decision. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 17
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: 18
□□ □ □□ □□ □□(BIA)□ □□□ □ □□□□ □□□□ □□□□□?
A. □□ □□□ □□ □□□ □□□ □□ □□
B. □□ □□□ □□□□ □ □□ □□□□ □□
C. □□ □□ □□
D. □□□□□ □□□ □□□□
Answer: (SHOW ANSWER)
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: 19
IT □□ □□□ □□□ □ □□ □ □□□□ □□□ □□□□.
A. IT □□□□□□ □□□□□ □□□□□.
B. □□ □□□ □□ □□ □□□ □□□□ □□□□.
C. □□ □□ □□(KPIs)□ □□□□.
D. □ □□□ □□□□□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
The greatest concern when reviewing an IT strategic plan is B. The plan does not support relevant organizational goals. This is because an IT strategic plan should align and integrate the IT goals and objectives with the organization's overall strategy and vision, and ensure that IT supports and enables the business processes and functions1. If the IT strategic plan does not support relevant organizational goals, it may lead to:
Suboptimal or negative outcomes and value for the organization, as IT investments and initiatives may not align with the organization's priorities, needs, or expectations1.
Conflicts or inconsistencies between IT and business functions, as IT may not deliver the expected level of service, quality, or performance2.
Wasted or inefficient use of resources, as IT may spend time, money, or effort on projects or activities that are not relevant or beneficial for the organization2.

NEW QUESTION: 20
IS □□□□ □□□ 2□ □□□ □□□ □□□□□ □3□ □□□□□ □□□ □□□ □□□ □□ □□(SLA)□ □□□□ □□□□. □□ □ □□□□ □□ □□□□ □ □□□ □□□□ □?
A. □□ □□ □□(RTO)□ □□ □□ □□(ORP)□ □□□ □□□ □ □□□.
B. SLA□ 1□ □□ □□□□ □□□□□.

C. □□ □□□□ □□□□□ □□□□□□.
D. □□ □□ □□(RPO)□ □□□ □□ □□ □□(DRP)□ □□□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
The recovery time objective (RTO) has a longer duration than documented in the disaster recovery plan (DRP) should be of greatest concern to the auditor when reviewing a bank's SLA with a third-party provider that hosts the bank's secondary data center. This is because the RTO is the maximum acceptable time for restoring a system or an application after a disaster or a disruption. A longer RTO than the DRP means that the bank may not be able to resume its critical business operations within the expected time frame, which may result in significant financial losses, reputational damage, customer dissatisfaction, or regulatory non- compliance12.
The SLA has not been reviewed in more than a year is not the greatest concern, although it is a good practice to review and update the SLA periodically to ensure that it reflects the current business needs and expectations, as well as any changes in the service provider's capabilities or performance. However, a lack of review does not necessarily imply a lack of compliance or quality of service, as long as the SLA is still valid and enforceable34.
Backup data is hosted online only is not the greatest concern, although it may pose some security risks if the backup data is not encrypted or protected by adequate access controls. Online backup data means that the backup data is stored on a remote server that can be accessed via the Internet, which may offer some advantages such as faster recovery, lower cost, and higher availability than offline backup data that is stored on physical media such as tapes or disks. However, online backup data also requires reliable network connectivity and bandwidth, as well as proper security measures to prevent unauthorized access or tampering56.
The recovery point objective (RPO) has a shorter duration than documented in the DRP is not the greatest concern, although it may indicate some inconsistency or misalignment between the SLA and the DRP. The RPO is the maximum acceptable amount of data loss measured in time from a disaster or a disruption. A shorter RPO than the DRP means that the bank may lose less data than expected, which may be beneficial for its business continuity and recovery. However, a shorter RPO may also imply more frequent backups, which may increase the cost and complexity of the backup process

NEW QUESTION: 21
IS □□□□ □□ □□□ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □□ □□□□. □□□□ □□ □ □□ □□ □□□ □□ □□□□ □□□□ □□□?
A. □□□ □□□ □□□□□□ □□□□.
B. □□□ □□□□ □□ □□□□ □□□□.
C. □□ □□□□□ □□□□□ □□□□□.
D. □□ □□□□□□ □□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)

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: 22
IS □□□□ □□ □□□ □□□ □□□ □□□□ □□ □□□ □□ □□ □□□□ □□□ □ □□□□. □□□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□ □□□ □□□□□ □□□ □□□□□.
B. □□ □□□ □□□ □□□□□□□.
C. □□ □□□ □□ □□□□ □□□□□.
D. □□□ □□ □□□ □□□□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 23
□□□□□ □□□□ □□ □□□ □ □□□ □□ □□□ □□□□□□ □□ □□□□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□□ □□ □□□(UAT) □□
B. □□ □□□ □□
C. □□ □□□□ □□
D. □□ □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
□□□□□□ □□ □□□ □□□□ □□ □□□ □□ □□□ □□□□□. □□ □ □□ □ □ □□□ □ □□□ □□ □ □□□ □□□□□?
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: 25
IS □□□□ □□□□□ □□□□□ □□□□ □□□□ □□□□. □ □□□ □□ □□ □ □□ □□□ □□ □□ □□ □ □□ □ □□ □□□ □□□□□?
A. □□ □□ □□□ □□ □□
B. □□□ □□□□ □□□ □□□ □ □□
C. □□ □□□ □□ □□
D. □□ □□□ □□□□
Answer: (SHOW ANSWER)
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: 26
IS □□□□ SaaS(Software as a Service) □□□□□ □□□□ □□ □□□□□ □□ □□ □ □□□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□□ □□□□□.
B. □□ □□□ □□□□□.
C. □□□□ □□ □□(BIA) □□
D. □□□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Before selecting a SaaS vendor, the most important action is to complete a risk assessment. A risk assessment is a process of identifying, analyzing, and evaluating the potential risks associated with outsourcing software and IT infrastructure to a third-party provider. A risk assessment helps to determine the impact and likelihood of various threats, such as data breaches, service disruptions, vendor lock-in, compliance issues, and legal disputes. A risk assessment also helps to identify the mitigation strategies and controls that can reduce or eliminate the risks.
A risk assessment is more important than determining service level requirements, performing a business impact analysis (BIA), or conducting a vendor audit because it provides the basis for these other actions.
Service level requirements are the expectations and obligations that define the quality and quantity of service that the vendor must provide to the customer. A BIA is a process of assessing the potential effects of an interruption or disruption of critical business functions or processes due to an incident or disaster. A vendor audit is a process of verifying the vendor's compliance with the contract terms, service levels, security policies, and best practices.
Service level requirements, BIA, and vendor audit are all important actions for selecting a SaaS vendor, but they depend on the results of the risk assessment. For example, service level requirements should reflect the risk appetite and tolerance of the customer, which are determined by the risk assessment. A BIA should prioritize the recovery of the most critical and vulnerable business functions or processes, which are identified by the risk assessment. A vendor audit should focus on the areas of highest risk and concern, which are highlighted by the risk assessment.
Therefore, an IS auditor should recommend to management that completing a risk assessment is the most important action before selecting a SaaS vendor.
References:
SaaS checklist: Nine factors to consider when selecting a vendor
SaaS vendor management: 10 best practices to achieve success
Best Practices for Software SaaS Vendor Selection and Negotiation
How to Evaluate SaaS Providers and Solutions by Developing ... - Gartner

NEW QUESTION: 27

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

A. □□□ □□□ □□□ □□□

B. □□□ □□□ □□ □□□ □□ □□

C. □□ □□□ □□ □□□ □□□

D. □□□ □□ □□□□ □□ □□ □□

Answer: A (LEAVE A REPLY)

The best way to prevent data leakage from a lost mobile device is data encryption on the mobile device. Data encryption is a technique that transforms data into an unreadable format using a secret key or algorithm. Data encryption protects data from unauthorized access or disclosure in case of loss or theft of a mobile device.

Complex password policy for mobile devices, triggering of remote data wipe capabilities, and awareness training for mobile device users are useful measures to enhance data security on mobile devices, but they do not prevent data leakage as effectively as data encryption. A complex password policy can be bypassed by brute force attacks or password cracking tools. Remote data wipe capabilities depend on network connectivity and device power availability. Awareness training for mobile device users can reduce human errors or negligence, but it cannot guarantee compliance or behavior change.

References: CISA Review Manual (Digital Version): Chapter 5 - Information Systems Operations and Business Resilience

NEW QUESTION: 28

□□ □□□□ □□ □□ □□□□□□□ □□□□□ □□□□ □□□ □□□□□ □□□ □ 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: 29
□□ □ □□ □□□(IoT) □□□ □□□□ □□□ □□□□□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□ □□□ □□ □ □□□□
B. □□ □□ □□ □□□ □□ □□□ □□ □□
C. □□ □□□□ □□
D. □□□□ □□□□□□ □□□□□ □□□□ □□□□□□□.
Answer: C (LEAVE A REPLY)

Changing default passwords is a critical security measure for IoT devices. Many IoT devices come with default credentials that are widely known and easily exploitable by attackers. Ensuring that these default passwords are changed to strong, unique passwords significantly reduces the risk of unauthorized access.
While logging, monitoring, firmware compliance, and network diagram reviews are important security practices, they are secondary to the fundamental step of securing device access through strong authentication.
References:
* ISACA CISA Review Manual, 28th Edition, Chapter 5: Protection of Information Assets.

NEW QUESTION: 30
□□□□ □□(□: □□□)□ □□ IP □□□ □□□ □ □□ □□ □□□ □□□□ □□ □ □□□ □□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□□ □□ □ □□□□□?
A. □□□ □□ □□□ □□□□
B. □□□ □□□□ □□□□
C. □□ □ □□□ □□□□
D. □□ □□ □□□□/□□□ □□□□(TCP/IP)
Answer: (SHOW ANSWER)

NEW QUESTION: 31
□□□ □□□□ □□ □□□ □□□□□□□ □□ □□□□□ □□□□ □□□ □□□□ □□. □□□ □□□ □□□ □□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□ □□□□□.
B. □□□□ □□□□ □□□ □□□ □□□□ □□
C. □□ □□□□□ □□□ □□□□□.
D. □□ □□ □□□(IDS)□ □□□□□□
Answer: B (LEAVE A REPLY)
The primary purpose of creating a simulated production environment with multiple vulnerable applications is to attract attackers in order to study their behavior. This is a technique known as honeypotting, which is a form of deception security that lures attackers into a fake system or network that mimics the real one, but is isolated and monitored1. Honeypotting can help security teams to learn about the attackers' methods, tools, motives, and targets, and to collect valuable intelligence that can be used to improve the security posture of the organization1. Honeypotting can also help to divert the attackers' attention from the real assets and to waste their time and resources2.
The other options are not the primary purpose of creating a simulated production environment with multiple vulnerable applications. To collect digital evidence of cyberattacks, security teams would need to use forensic tools and techniques that can preserve and analyze the data from the compromised systems or networks3. To provide training to security managers, security teams would need to use simulation tools and scenarios that can test and enhance their skills and knowledge in responding to cyber

incidents4. To test the intrusion detection system (IDS), security teams would need to use penetration testing tools and methods that can evaluate the effectiveness and performance of the IDS in detecting and preventing malicious activities5.
References:
What is a Honeypot? | Imperva
Honeypots: A sweet solution for identifying intruders | CSO Online
Digital Forensics - an overview | ScienceDirect Topics
Cybersecurity Training & Exercises - Homeland Security
What is Penetration Testing? | Types & Stages | Imperva

NEW QUESTION: 32
□□ □ POS(□□ □□ □□) □□□□□ □□□□ □□ □□□□ □□□□ □□□□ □□ □□ □□ □□ □□ □□ □□□ □□□□□?
A. □□□
B. □□ PIN
C. □□
D. □□□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
□□ □□□□ □□□ □ □□ □□ □□ □ □□ □□□□□?
A. □□ □□ □□(NDA)□ □□□□□.
B. □□□ □□ □□ □□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□ □□□□.
Answer: (SHOW ANSWER)
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: 34
□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□□□ □ □ IS □□□□ □□ □□ □□ □ □□□ □□□□□?
A. □□□□□ □□□□□□ □ □ □□□□.
B. □□□ □□ □□□□□□ □□ □□□ □□□ □ □□□□.
C. □□ □□□ □□□ □□□ □ □□□□.
D. □□ □□□□ □□ □□□ □□□□ □□ □□ □□□□.
Answer: (SHOW ANSWER)
The greatest concern for an IS auditor when an international organization intends to roll out a global data privacy policy is that local regulations may contradict the policy. Data privacy regulations vary across different countries and regions, and they may impose different or conflicting requirements on how personal data can be collected, processed, stored, transferred, and disclosed. The organization should ensure that its global data privacy policy complies with the applicable local regulations in each jurisdiction where it operates, or risk facing legal sanctions or reputational damage. Requirements may become unreasonable, but this is not a major concern for an IS auditor, as it is a business decision that should be based on a cost-benefit analysis. The policy may conflict with existing application requirements, but this is not a serious concern for an IS auditor, as it can be resolved by modifying or updating the applications to align with the policy. Local management may not accept the policy, but this is not a critical concern for an IS auditor, as it can be mitigated by providing adequate training and awareness on the policy and its benefits. References:
* CISA Review Manual, 27th Edition, pages 406-4071
* CISA Review Questions, Answers & ExplanationsDatabase, Question ID: 2592

NEW QUESTION: 35
□□□ □□□□□□ □□□□(EA) □□□□□ □□□□ IS □□□□ □□ □ □□ □□□ □ □ □□□ □□□□□?
A. IT □□□□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□□.
B. □□□□ □□ □□□□ □□□ CIO□□□.
C. □□ □□ □□ □□□ EA □□□□□□ □□□□□.
D. EA □□□□□ IT□ □□□ □□ □□□□□ □□□□□.
Answer: A (LEAVE A REPLY)

Comprehensive and Detailed Step-by-Step Explanation:
Enterprise Architecture (EA) governance requires proper oversight and separation of duties to ensure strategic alignment and risk management.
* Option A (Correct):If IT application owners have sole authority over architecture approval, there is a high risk of inadequate governance, lack of strategic alignment, and potential conflicts of interest.
Architecture decisions should involve multiple stakeholders, including business and security teams, to ensure compliance, security, and business alignment.
* Option B (Incorrect):While having the CIO chair the architecture review board might not be ideal, it is not thegreatestconcern. The CIO is a senior leader who can provide oversight and direction, even if additional governance mechanisms should be in place.
* Option C (Incorrect):Reviewing security requirements within the EA program is abest practice, as it ensures that security is embedded into enterprise architecture rather than treated as an afterthought.
* Option D (Incorrect):Enterprise architecture should ideally encompass both IT and business processes.
Governing non-IT-related projects is not inherently problematic, as EA is designed to align business strategy with IT infrastructure.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Covers IT governance and EA program structure.

NEW QUESTION: 36
IS □□□□ □□□□□ □□□ □□□□□□□ □□ □□□ □□□ □□□□□ □□□ □ □ □□□ □□ □□□□□.
□ □□□□ □□ □ □□ □□□ □□ □ □□□□□?
A. □□□ □□
B. □□□ □□ □□ □□□ □□□
C. □□ □ □□ □□(MTBF) □□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
The greatest concern with this situation is that a business-critical application does not currently have any level of fault tolerance and thus has a single point of failure. A single point of failure is a component or element of a system that, if it fails, will cause the entire system to stop functioning. Fault tolerance is the ability of a system to continue operating without interruption or degradation in the event of a failure of one or more of its components or elements. Fault tolerance can be achieved by using techniques such as redundancy, replication, backup, or failover. A business-critical application should have a high level of fault tolerance to ensure its availability, reliability, and continuity. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.51
* CISA Online Review Course,Domain 3, Module 3, Lesson 22

NEW QUESTION: 37
□□□ □□□ □□□ 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: 38
□□ □ □□ □□□ □□□ □□ □□ □ IS □□□□ □□ □□□□ □ □□ □□□□□?
A. □□ □□□ □□□□ □□□ □□□□□ □□ □□ □□□ □□□□.
B. □□□ □□□□ □□□ □□□ □□ □□ □□□□.
C. □□□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□ □□□□□.
D. □□ □□□ □□□□□ □□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
□□ □□□ □□□ □□□□ □□□ IS □□□□ □□□□ □□ □□□ IT □□□□ □□□ □□□ □□□□□□. □□□□□□ □□□ □□□□ □ □□ □□□ □□ □□ □□ □ □ □ □ □□□□?
A. IT □□ □ □□□□ □□ □□ □□ □□□
B. □□□□□ IT □□ □□□□ □□□
C. □□ □3□ IS □□ □□□
D. □□ □ □□ □□ IS □□ □□□
Answer: (SHOW ANSWER)
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: 40
□□ □ □□□□□ □□ □□□ □□□□?
A. □□□□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□ □ □□□□□.
B. □□□ □□□ □□□ □□□□ □□ IP □□□ □□□□□ □□□□□ □□□□□□□.
C. □□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□□ □□□□ □□ □□□□ □ □□□□□.
D. □□□□ □□□□□ □□ □□□ □□□ □□□ □□□□ □□□□ □3□□□ □□□ □□.
Answer: (SHOW ANSWER)
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: 41
□□ □ □□ □ □□□ □□□□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□ □
B. □□ □□
C. □□□□ □□
D. □□ □□ □□ □□
Answer: A (LEAVE A REPLY)
The best point in time to conduct a post-implementation review is after a full processing cycle. A post- implementation review is a process to evaluate whether the objectives of the project were met, how effective the project was managed, what benefits were realized, and what lessons were learned. A post-implementation review should be conducted after a full processing cycle, which is the period of time required for a system or process to complete all its functions and produce its outputs. This allows for a more accurate and comprehensive assessment of the project's performance, outcomes, impacts, and issues. The other options are not as good as option A. Conducting a post-implementation review immediately after deployment is too soon, because it does not allow enough time for the project's product or service to operate in the real world and generate measurable results.

Conducting a post-implementation review after the warranty period is too late, because it may miss some important feedback or opportunities for improvement that could have been addressed earlier. Conducting a post-implementation review prior to the annual performance review is irrelevant, because it does not align with the project's life cycle or objectives. References: What is Post-Implementation Review in Project Management?, What Is the Post- Implementation Review (PIR) Process?, Post-implementation review in project management?

NEW QUESTION: 42

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

A. □□ □□□ □□□□ □□ □□ □□□ □□□ □□

B. □□ PIN □□ □□

C. □□□□ □□ □□□ □□□□ □□□ □□

D. □□□□ □□□□(CCTV) □□

Answer: C (LEAVE A REPLY)

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: 43
□□ □ □□ □□□ □□ □□□ □□□ □□□□ □□ □ □□□□□ □□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□ □ □□ □□□□□?
A. □□□ □□□
B. □□ □□□
C. □□ □□□
D. □□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 44
□□ □□ □□ □□ □□□□ □□□□□ □□ □□□ □□ □□□□ □□□□□. □□ □ IS □□□□ □□□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□ □□□□□.
B. □□ □□□□□ □□□□ □□□ □□□□□.
C. □□ □□□□ □□□ □□□ □□□□□ □□□ □□□ □□□□□.
D. □□□ □□□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 45
□□□ □□ □□ □□□ □□□□ □□□ □ IS □□□□ □□□ □ □□ □□ □□ □□ □ □□ □□ □ □□ □□□□?
A. □□□□ □□□□ □□
B. □□ □□□ □□
C. □□□ □□ □□
D. □□ □□□□
Answer: C (LEAVE A REPLY)
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: 46
□□ □ IT □□□□□ □□□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□□ □□ □□ □□
B. □□ □□□□ □□
C. □□□□ □□ □□
D. □□□□ □□
Answer: C (LEAVE A REPLY)
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: 47
□□□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□ □□□□ □□ □□
B. □□□□ □□□□ □□ □□
C. □□□ □□□ □□ □□□ □□
D. □□□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
□□ □□□ □□□(EUC)□□ □□□ □□□□ □□□ □ □□ □ □□□ □□□□□?
A. □□□□ □□□□ □□ □ □□□□.
B. □□□□ □□□□□ □□□□ □□ □ □□□□.
C. □□□□ □□ □□□□ □□ □ □□□□.
D. □□ □□□□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)
End-user computing (EUC) is a system in which users are able to create working applications besides the divided development process of design, build, test and release that is typically followed by software engineers1. Examples of EUC tools include spreadsheets, databases, low-code/no-code platforms, and generative AI applications2. EUC tools can provide flexibility, efficiency, and innovation for the users, but they also pose significant risks if not properly managed and controlled3.
The greatest risk when relying on reports generated by EUC is that the data may be inaccurate. Data accuracy refers to the extent to which the data in the reports reflect the true values of the underlying information4.
Inaccurate data can lead to erroneous decisions, misleading analysis, unreliable reporting, and compliance violations. Some of the factors that can cause data inaccuracy in EUC reports are:

Lack of rigorous testing: EUC tools may not undergo the same level of testing and validation as IT-developed applications, which can result in errors, bugs, or inconsistencies in the data processing and output3.
Lack of version and change control: EUC tools may not have a clear record of the changes made to them over time, which can create confusion, duplication, or loss of data. Users may also modify or overwrite the data without proper authorization or documentation3.
Lack of documentation and reliance on end-user who developed it: EUC tools may not have sufficient documentation to explain their purpose, functionality, assumptions, limitations, and dependencies. Users may also rely on the knowledge and expertise of the original developer, who may not be available or may not have followed best practices3.
Lack of maintenance processes: EUC tools may not have regular updates, backups, or reviews to ensure their functionality and security. Users may also neglect to delete or archive obsolete or redundant data3.
Lack of security: EUC tools may not have adequate access controls, encryption, or authentication mechanisms to protect the data from unauthorized access, modification, or disclosure. Users may also store or share the data in insecure locations or devices3.
Lack of audit trail: EUC tools may not have a traceable history of the data sources, inputs, outputs, calculations, and transformations. Users may also manipulate or falsify the data without detection or accountability3.
Overreliance on manual controls: EUC tools may depend on human intervention to input, verify, or correct the data, which can introduce errors, delays, or biases. Users may also lack the skills or training to use the EUC tools effectively and efficiently3.
The other options are not as great as data inaccuracy when relying on EUC reports. Reports may not work efficiently, reports may not be timely, and historical data may not be available are all potential risks associated with EUC tools, but they are less severe and less frequent than data inaccuracy. Moreover, these risks can be mitigated by improving the performance, scheduling, and storage of the EUC tools. However, data inaccuracy can have a pervasive and lasting impact on the quality and credibility of the reports and the decisions based on them. Therefore, option A is the correct answer.
References:
What is Data Accuracy?
What Is End User Computing (EUC) Risk?
End-user computing
End-User Computing (EUC) Risks: A Comprehensive Guide

NEW QUESTION: 49
□□ □ IT □□□□□□ □□□ □□□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. IT □□□□ □□□□ □□□□ □□□ □□ □□ □□□ □□□ □□□ □□
B. □□□□□ □□□ □□□□□ □□ □□□ □□ □□□
C. □□□□ □□ □ □□ □□ □□ □□ □□ □□□ □□
D. □□ □ □□ □ □□□□□ □□ □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 50
□□□ □□□□ □□□ □□(BCP)□ □□□ □□□□ □ □□□ □□ □□□ □□ □□□ □□□ □□□ □ IS □□□□ □□□□□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□
B. □□□ □□□ □□
C. □□□ □□□□ □□□□
D. □□ □□ □□□□
Answer: (SHOW ANSWER)
The best way to assess the effectiveness of changes made to processes and tools related to an organization's BCP is to review the full test results of the BCP. Full test results can provide evidence of whether the changes have improved the BCP's objectives, such as recovery time objectives (RTOs), recovery point objectives (RPOs), and business impact analysis (BIA). The other options are not as effective as reviewing the full test results, as they do not demonstrate the actual performance of the BCP under simulated disaster scenarios.
Completed test plans are only documents that outline the scope, objectives, and procedures of the BCP testing, but they do not show the outcomes or issues encountered during the testing. Updated inventory of systems is a component of the BCP that identifies the critical systems and resources required for business continuity, but it does not measure the effectiveness of the BCP changes. Change management processes are controls that ensure that changes to the BCP are authorized, documented, and communicated, but they do not evaluate the impact or benefit of the changes. References: CISA Review Manual (Digital Version), Chapter 4, Section 4.2.3

NEW QUESTION: 51
IS □□□ □□ □□-□□ □□, □□□ □□□, □□□ □□□□ □□ □□□□□. □□ □□ □ □□ □□□□□.
A. □□ □□□□□
B. □□ □□□
C. □□ □□ □□
D. □□ □□ □□(CSA)
Answer: B (LEAVE A REPLY)
A 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.
A 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 other options are not the primary uses of a 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.

NEW QUESTION: 52
□□□ □□□ □, □□□□ □□ □□□ □□□□□ □ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□ □□
B. □□□□□□
C. □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 53
IS □□□□ □□□□ □□□□□□ □□□□ □□□□. □□ □ □□□□ □□□□□ □□ □□ □□□ □□□□□?
A. □ □□□□ □□ □□□□ □□□/□□ □□
B. □□ □□□ □□ □□□□ □□□□□ □□□□
C. □□ □□ □□ □□□□(VLAN) □
D. □□□□□(DMZ) □□
Answer: (SHOW ANSWER)

NEW QUESTION: 54
□□ □ □□□ IT □□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. IT □□ 1□□ □□ □□ □ □□ □□
B. □□ □□ □ □□□ □□ □□ □□ □□
C. □□□ IT □□□ □□□□ □□□ □□□□□□ □□□□ □ □□□ □□ □□
D. □□□ □□□ □□□ □□□ IT □□ □□□ □□ □□□ □□
Answer: (SHOW ANSWER)
The metric that would best measure the agility of an organization's IT function is average time to turn strategic IT objectives into an agreed upon and approved initiative. IT agility is the ability of an IT function to respond quickly and effectively to changing business needs and opportunities. By measuring how fast an IT function can translate strategic IT objectives into actionable initiatives, such as projects or programs, an organization can assess how well its IT function can align with and support its business strategy. Average number of learning and training hours per IT staff member, frequency of security assessments against the most recent standards and guidelines, and percentage of staff with sufficient IT-related skills for the competency required of their roles are metrics that may indicate other aspects of IT performance, such as capability development, security maturity, and skills gap analysis, but they do not directly measure IT agility. References: ISACA Journal Article: Measuring IT Agility

NEW QUESTION: 55
□□ □□ □□□ □□ □□ □□□ □□□□ □□ IS □□□□ □□□ □□□ □□□□ □ □ IT □□□ □□ □□□ □□□ □□□□□□. □□ □ □□□□ □□□ □□□ □□□□ □?
A. □□ □□ □□□ □□□□□ □□ □□□ □□□ □□□.
B. □□ □□ □□□□ □□□ □□□ □□□ □□□□□.
C. □□ □ □□ □□ □□□ □□□ □□□ □□□□.
D. □□□ □□ □□□ □□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
□□□ □□ □□ □□(SDLC)□ □□□□ IS □□□□ □□□□ □□□ □□ □□ □□□ □□□ □□ □□□□□□. □□ □ □□□ □□ □ □□ □□□ □□ □□ □□□□□?
A. □□□□ □□ □□□ □□□ □□□□ □□□□□.
B. □□□□ □□□□ □□□□ □□□□ □□□□□.
C. □□□□□ □□□□ □□□ □□□□ □□□□ □□□□□.
D. □□□□ □□□ □□□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 57
□□ □ □□□□□ □□□□□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□□ □ □ □□ □□□ □□□□□?
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: 58
□□ □ □□ □□ □□□ □□□□ □□□ □□□□□□ □□□□□ □□□ □□ □ □□ □□ □□□□ □□ □□□ □□□□□ □□ □ □□ □□□ □□□?
A. □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□ □□□ □□□□□.
B. □□□ □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □ □□ □□□ □□□□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□□ □□□□□□ □□□□□.
Answer: (SHOW ANSWER)
The best way to ensure that potential security issues are considered by the development team as part of incremental changes to agile-developed software is to include a mandatory step to analyze the security impact when making changes. This will help to identify and mitigate any security risks or vulnerabilities that may arise from the changes, and to ensure that the software meets the security requirements and standards. The other options are not as effective, because they either delegate the security analysis to someone outside the development team, rely on post-deployment testing, or focus on documentation rather than analysis. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.5

NEW QUESTION: 59
□□□ □□□□□□□ □□□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□
B. □□□□ □ □□ □□
C. □□ □□□ □□□ □□
D. □□□□□□ □□ □□
Answer: B (LEAVE A REPLY)
Visualization technology is the use of software and hardware to create graphical representations of data, such as charts, graphs, maps, images, etc. Visualization technology can help users to understand, analyze, and communicate complex and large amounts of data in an intuitive and engaging way1.
One of the primary advantages of using visualization technology for corporate applications is that it can improve the utilization of resources, such as time, money, human capital, and physical assets. Some of the ways that visualization technology can achieve this are:
* Visualization technology can help users to quickly and easily explore, filter, and interact with data, reducing the need for manual data processing and analysis1. This can save time

and effort for both data producers and consumers, and allow them to focus on more value-added tasks.
* Visualization technology can help users to discover patterns, trends, outliers, correlations, and causations in data that may otherwise be hidden or overlooked in traditional reports or tables1. This can enable users to make better and faster decisions based on data-driven insights, and optimize their strategies and actions accordingly.
* Visualization technology can help users to communicate and share data more effectively and persuasively with different audiences, such as customers, partners,investors, regulators, etc1. This can enhance the reputation and credibility of the organization, and foster collaboration and innovation among stakeholders.
* Visualization technology can help users to monitor and measure the performance and impact of their activities, products, services, or processes1. This can help users to identify problems or opportunities for improvement, and adjust their plans or actions accordingly.
* Visualization technology can help users to create engaging and interactive experiences for their customers or end-users1. This can increase customer satisfaction and loyalty, and generate more revenue or value for the organization.
Therefore, using visualization technology for corporate applications can help organizations to better utilize their resources and achieve their goals.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* TechRadar Blog, Best data visualization tools of 20232
* IBM Blog, What is Data Visualization?3
* TDWI Blog, Data Visualization Technology4
* Tableau Blog, What are the advantages and disadvantagesof data visualization?

NEW QUESTION: 60
□□□ □□□□ □□□□□ □□□ □ IS □□□□ □□ □□□□ □□□□ □ □□□ □ □□□□?
A. □□ □□□□□□ □□ □□□ □□□ □□ □□□ □□□ □□□ □□
B. □□□ □□□□□ □□□□ □□□ □□
C. □□□□□ □3□ □□□ □□□□□ □□□□ □□ □□□□ □□□ □□
D. □□□□ □□□ □□ □□□□ □□□ □□□ □□□□
Answer: B (LEAVE A REPLY)
The most important thing for an IS auditor to examine when reviewing an organization's privacy policy is its legitimate purpose for collecting personal data. A legitimate purpose is a clear and specific reason for collecting personal data that is necessary for the organization's business operations or legal obligations, and that respects the rights and interests of the data subjects. A legitimate purpose is the basis for establishing a lawful and fair processing of personal data, and it should be communicated to the data subjects

in the privacy policy. The other options are not as important as the legitimate purpose in reviewing the privacy policy.
Explicit permission from regulators to collect personal data is not always required, as there may be other lawful bases for data collection, such as consent, contract, or public interest. Sharing of personal information with third-party service providers is not prohibited, as long as there are adequate safeguards and agreements in place to protect the data. The encryption mechanism selected by the organization for protecting personal data is a technical control that can enhance data security, but it does not determine the legality or fairness of data collection. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION: 61
□□□□ □□ □□□(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: 62
□□□□□ □□ □□□ 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: 63
□□□ IT □□□□ □□□□ IS □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□ □□□□ □□ □□□□□ □□ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□□ □?
A. □□□ □□ □□ □□(ERP) □□□
B. □□□□□□ □□□□(EA) □□
C. □□□ □□□ □□□
D. □□□□□ □□ □□ □□
Answer: B (LEAVE A REPLY)

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

The most significant risk from this observation is that access rights may not be removed in a timely manner. If the process for removing access for terminated employees is not documented, there is no clear guidance or accountability for who, how, when, and what actions should be taken to revoke the access rights of the employees who leave the organization. This could result in delays, inconsistencies, or omissions in removing access rights, which could allow terminated employees to retain unauthorized access to the organization's systems and data. This could compromise the security, confidentiality, integrity, and availability of the information assets. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 65
□□□ □□ □□□ □□□□ □□ □□□ □□ □□ □□(SDLC)□ □□ □□□ □□□ □ □□□□□. □□ □ □□□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□□□ □□ □□□□ □□□ □□□□□ □□□□□□.
B. □□□□□ □□□ □□□□ □□□ □□□ □□□□□.
C. □□ □□□ □□□ □□□□ □□□ □□□□□.
D. □□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 66
□ □□ □□□ □□□ □□ □□ □□□□□ □□□□ □□□□ IS □□□□□ □□ □ □ □□□ □□ □ □□ □□□□?
A. □ □□□ □□□ □□□□□□ □□□□.
B. □□ □□□ □□(BCP)□ □□ 6□□ □□ □□□□□ □□□□□.
C. □□□□ □□ □□□□ □□□□ □□□□□.
D. □□□□ □□□□□□□ □ □□□ □□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
□□ □□□ □□ 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: 68
IT □□□□ □□ □□□ □□□ □□□□□ □□ IS □□□□ □□□ □□□ □□□ □□□ □□□. □□ □ □□□□ □□ □□ □□□ □□□□□ □□□?
A. □□ □□□□□ □□□□.
B. □□-□□ □□□ □□□□□.
C. □□□□□□ □□□□□ □□□ □□□□□.
D. □□ □□ □□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
□□ IT □□□□□□ □□□ □□□ □□ □□ □□□ □□□□ □, IS □□□□ □□ □□ □□□ □□ □ □□ □□ □□ □□□□ □□ □ □□ □□□?
A. □□□□ □□□ □□ □□ IT □□□□□□ □□□□□.
B. □□□□ □□□ □□ □□ IT □□□□□□ □□□□□□.
C. IT □□□□□□ □□ □□ □□□(ROI)□ □□□□□□.
D. IT□ □□ □□ □□(KPI)□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 70
□□ □ Agile □□ □□□□ □□□□ □□ □ □□□ □□□□□?
A. □□□ □□ □□ □□
B. □□ □□ □□
C. □□□□□ □□ □□□ □ □□□
D. □□ □□□ □□□□ □ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
□□ □□□□ □□□ □□ □□□ □□ □□ □□ □□□ □□□□ □ □□□□ □□□ □ □ □□ □□□□ □□□□ □□, IS □□□□ □□ □ □□ □□ □□ □□□ □□ □ □□ □□□?
A. □ □ □□ □□□ □□□□ □□ □□□□ □□□□□□.
B. □□□ □□ □□ □□ □□□ □□□□□ □□□□□.
C. □□□ □□□ □□□□□□ □□□□□.
D. □□ □□ □□□ □□□□□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
□□ □□□□□□ □□□ □□ IS □□ □□□ □□□□□.
A. IS □□ □□□ □□□ □□□ □□□□□.
B. □□ □□□□□ □□□□ □□□ □□ □□□□ □□.
C. □□ □□□ □□□ □□ □ □□□ □□□□□.
D. □□□ □□□□ □ □□□ □□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Audit frameworks can assist the IS audit function by providing direction and information regarding the performance of audits. Audit frameworks are sets of standards, guidelines, and best practices that help IS auditors plan, conduct, and report on their audit engagements. Audit frameworks can help IS auditors ensure the quality, consistency, and professionalism of their audit work, as well as comply with the expectations and requirements of the stakeholders and regulators. Audit frameworks can also help IS auditors address the specific challenges and risks of auditing information systems and technology.
Defining the authority and responsibility of the IS audit function is not a way that audit frameworks can assist the IS audit function, but rather a way that the IS audit charter can assist the IS audit function. The IS audit charter is a document that defines the purpose, scope, objectives, and authority of the IS audit function within the organization. The IS audit charter can help IS auditors establish their role and position in relation to other functions and departments, as well as clarify their rights and obligations.
Providing details on how to execute the audit program is not a way that audit frameworks can assist the IS audit function, but rather a way that the audit methodology can assist the IS audit function. The audit methodology is a set of procedures and techniques that guide IS auditors in performing their audit tasks and activities. The audit methodology can help IS auditors apply a systematic and structured approach to their audit work, as well as use appropriate tools and methods to collect and analyze evidence.
Outlining the specific steps needed to complete audits is not a way that audit frameworks can assist the IS audit function, but rather a way that the audit plan can assist the IS audit function. The audit plan is a document that describes the scope, objectives, timeline, resources, and deliverables of a specific auditengagement. The audit plan can help IS auditors organize and manage their audit work, as well as communicate their expectations and responsibilities to the auditees.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 51 1
* Understanding Project Audit Frameworks - Wolters Kluwer 2
* How to Implement a Robust Audit Framework - Insights - Metricstream 3
* What Is The Internal Audit Function? An Accurate Definition Of The

NEW QUESTION: 73

□□ □ □□ □□□ □□(DDoS) □□□ □□□□ □□□ □□ □□ □ □□□ □ □□ □□ □□□□□?

A. □□ □□□ □□ □□

B. □□ □□ □□□□

C. □□ □□

D. □□ □□□

Answer: B (LEAVE A REPLY)

The best way to detect that a distributed denial of service (DDoS) attack is occurring is to use automated monitoring of logs. A DDoS attack disrupts the operations of a server, service, or network byflooding it with unwanted Internet traffic2. Automated monitoring of logs can help pinpoint potentialDDoS attacks by analyzing network traffic patterns, monitoring traffic spikes or other unusual activity, and alertingadministrators or security teams of any anomalies or malicious requests, protocols, or IP blocks3.

Automated monitoring of logs can also help identify the source, type, and impact of the DDoS attack, and provide evidence for further investigation or mitigation.

The other options are not as effective as automated monitoring of logs for detecting DDoS attacks. Customer service complaints are an indirect and delayed indicator of a DDoS attack, as they rely onusers reporting problems with accessing a website or service. Customer service complaints may also be caused by other factors unrelated to DDoS attacks, such as server errors or network issues. Server crashes are an extreme and undesirable indicator of a DDoS attack, as they indicate that the server has already been overwhelmed by the attack and has stopped functioning. Server crashes may also result in data loss or corruption, service disruption, or reputational damage. Penetration testing is a proactive and preventive measure for assessing the security posture of a system or network, but it does not detect ongoing DDoS attacks. Penetration testing may involve simulating DDoS attacks to test the resilience or vulnerability of a system or network, but it does not monitor real-time traffic or identify actual attackers.

References:

* ISACA CISA Review Manual 27th Edition (2019), page 254
* How to prevent DDoS attacks | Methods and tools | Cloudflare2
* Understanding Denial-of-Service Attacks | CISA3

NEW QUESTION: 74

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

A. □□ □□ □ □□□ □□□□ □□□□ □□□□□.

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

C. □□□□ □□□□ □□ □□□ □ □□□□.

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

Answer: B (LEAVE A REPLY)

The greatest concern for an IS auditor reviewing a network printer disposal process is that evidence is not available to verify printer hard drives have been sanitized prior to disposal. This can expose sensitive data to unauthorized parties and cause data breaches. Disposal policies and procedures not being consistently implemented or business units being allowed to dispose printers directly to vendors are compliance issues, but not as critical as data protection. Inoperable printers being stored in an unsecured area is a physical security issue, but not as severe as data leakage. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
387

NEW QUESTION: 75
□□□ □□ □□□□ □□ □□□ □□□□.
A. □□□□ □□□ □□□ □ □□ □□□ □□□□□.
B. □□□□ □□□□□ □□□□□.
C. □□ □ □□□ □□ □□□ □□□□□ □□□□□.
D. □□ □□□□□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
An organization's audit charter primarily describes the auditors' authority to conduct audits. The audit charter is a formal document that defines the purpose, scope, responsibilities, and reporting relationships of the internal audit function. It also establishes the auditors' right of access to information, records, personnel, and physical properties relevant to their work. The audit charter provides the basis for the auditors' independence and accountability to the governing body and senior management.

NEW QUESTION: 76
□□ □ □□□□ □□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□ □□□ □□□ □□□ □ □□□□.
B. □□□□ □□ □□□ □□□ □□ □□□ □□□ □□ □ □□□□.
C. □□ □□□ □□ □□□□□□ □□□ □ □□□□.
D. □□□ □□□□□ □□□ □□ □□□ □□ □□□ □□ □ □□□□.
Answer: B (LEAVE A REPLY)
A concern associated with virtualization is that performance issues with the host could impact the guest operating systems, which are the operating systems that run on virtual machines within the host. For example, if the host has insufficient memory, CPU, disk space, or network bandwidth, it could affect the performance and availability of the guest operating systems and the applications running on them. The physical footprint of servers could decrease within the datacenter, processingcapacity may be shared across multiple operating systems, and one host may have multiple versions of the same operating system are not concerns associated with virtualization, but rather benefits or features of virtualization that can help reduce costs, improve efficiency, and enhance flexibility. References: CISA Review Manual (Digital Version), Chapter 4:

Information Systems Operations and Business Resilience, Section 4.2: IT Service Delivery and Support

NEW QUESTION: 77
□□ □□ □□□(IDS)□ □□□ □□□ □ IS □□□□ □□□ □□ □□□ □□ □□□□ □□□.
A. □□□□□ □□□ □□□ □□□ □□□□□□.
B. □□ □□□ □□□□ □□□□□.
C. □□□ □□□□ □□□□□□.
D. □□ □□ □□□ □□□□□□□.
Answer: (SHOW ANSWER)
The main purpose of an IDS is to detect and report malicious or suspicious activity on a network or a host. If an IDS fails to identify actual attacks, it means that the IDS is not functioning properly or effectively, and it exposes the organization to serious security risks and potential damage. This is the most concerning scenario for an IS auditor, as it indicates a major deficiency in the IDS performance and configuration.
ReferencesWhat is an intrusion detection system (IDS)?What is Intrusion Detection Systems (IDS)?How does it Work?When reviewing an intrusion detection system (IDS), an IS auditor ...Intrusion Detection Systems (IDS)-An Overview with a Generalized ...An overview of issues in testing intrusion detection systems - NISTA Review of Intrusion Detection Systems and Their ...

NEW QUESTION: 78
□□ □ □□ □□□ □□□□□ □□□□ □□□ □ □□ □□□□ □□ □□□ □□□□ □?
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: 79
□□ □ □□□□ □□ □□ □□□□□ □□ □ □□□ □□□ □□□ □□□□□?
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: 80
□□ □□ □ IS □□□□□ □□ □□ □□□ □ □□ □□□□ □□ □□ □□□□ □□ □ □ □□ □□□□ □□□□ □□ □□□□□?
A. □□ □□ □□
B. □□□ □□ □□ □□
C. □□ IT □□□ □□□
D. IT □□□□□ □□□ □□
Answer: D (LEAVE A REPLY)
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: 81
□□ □□□ □□ □□□□ □□ □□□ □□□ □□□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□ □ □□□ □□□□□.
B. □□ □□□ □□□ □□ □□□ □□□□□.
C. □□□ □□□□ □□ □ □□□ □□□□□.
D. □□ □□□ □□ □□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)
The data retention policy for a global organization with regional offices in multiple countries should align with local laws and regulations, as they may vary significantly from one country to another and may impose different requirements and penalties for non-compliance. The policy should also consider the corporate policies and practices, the global best practices, and the business goals and objectives, but these are secondary to the legal compliance. References: CISA Review Manual (Digital Version), Chapter 5: Protection of InformationAssets, Section 5.3: Data Classification and Protection

NEW QUESTION: 82
IS □□□□ □□□ □□ □□□ □□(BCP)□ □□ □□□ □□ □□□ □□□□□ □□□.
□□ □ □□□□□ □□ □□□ □□ □□ □□□□□?
A. □□ □□ □□(DRP) □□□ □□
B. □□ □□ □□(BIA)

C. □□ □□□ □□ □□
D. □□ □□ □□(KPI)
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
To ensure that theBCP aligns with business strategy, aBusiness Impact Analysis (BIA)is the most valuable resource.
* Option A (Incorrect):DRP testing resultsshow how wellsystems recover, but they do notestablish strategic alignmentwith business priorities.
* Option B (Correct):ABIA identifies critical processes, financial impact, and business priorities, ensuring that theBCP is alignedwith strategic goals.
* Option C (Incorrect):Thecorporate risk management policyis broader and does not focus on business continuity priorities.
* Option D (Incorrect):KPIs measure performance, but they do notdefine business continuity needs.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- CoversBCP, BIA, and business continuity alignment.

NEW QUESTION: 83
□□ □ □□□□ □□ □□(B1A)□ □□□□ □ □□ □□□ □□□ □□□□ □□ □□□ □□?
A. □□ □□□□ □□□□□ □□□□
B. □□□□ □□
C. □□□□□□ □□ □□
D. □□ □□ □□ □□□ □□
Answer: A (LEAVE A REPLY)
A business impact analysis (BIA) is a process that identifies and evaluates the potential effects of disruptions to critical business operations as a result of a disaster, accident or emergency. A BIA should include an inventory of relevant business processes that support the organization's strategic objectives and are essential for its continuity. The inventory should also identify the dependencies, interdependencies, recovery priorities and time frames for each business process. Policies for business procurement, documentation of application configurations and results of business resumption planning efforts are not as useful as an inventory of relevant business processes for performing a BIA. References:
* : Business Impact Analysis (BIA) Definition
* : Business Impact Analysis (BIA) | ISACA

NEW QUESTION: 84
IT □□□ □□□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□□□?
A. □□□
B. ITC □□□
C. □□ □□□

D. □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 85

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

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

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

C. □□ □□□ □□□ □□□ □□ □□□ □□□□ □□□.

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

Answer: B (LEAVE A REPLY)

The statement that BEST demonstrates alignment with data classification standards related to the protection of information assets is D. All information assets will be assigned a clearly defined level to facilitate proper employee handling. Data classification involves categorizing information assets based on their sensitivity, importance, and usage. Assigning clearly defined levels (such as public, internal, confidential, etc.) to information assets ensures that appropriate security controls are applied based on their classification. By doing so, organizations can manage access, encryption, and other protective measures effectively12.

References:

1. IFRC. "Information Security: Acceptable Use Policy." 1(https://www.ifrc.org/sites/default/files/2021-11/IFRC-Information-Security-Acceptable-Use-Policy.pdf)
2. UNSW Sydney. "Data Classification Standard." 2(https://www.unsw.edu.au/content/dam/pdfs/governance/policy/2022-01-policies/datastandard.pdf)
3. Digital Guardian. "What is a Data Classification Policy?" 3(https://www.digitalguardian.com/blog/what- data-classification-policy)
4. Microsoft Service Trust Portal. "Data classification & sensitivity label taxonomy." 4(https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-classification-and-labels)
5. Clark University ITS Policies. "Data Classification - Data Security Policies." 5(https://www2.clarku.edu/offices/its/policies/data_classification.cfm)

NEW QUESTION: 86

□□□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□□ □□ □□□ □□□□ 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: 87
IS □□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□□ □□□ □□□□□□. □ □□□ □□□ □□□□ □□□ □ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□□□ □□□□□ □□ □□□□□.
B. □□□□ □□□□□ □□□□.
C. □□□ □□□ □□□□ □□ □ □□□□.
D. □□□ □□ □□□ □□□ □□□□□□□□□.
Answer: (SHOW ANSWER)
The most important thing for the auditor to confirm when sourcing the population data for testing accounts payable controls by performing data analytics is that the data is taken directly from the system. Taking the data directly from the system can help ensure that the data is authentic, complete, and accurate, and that it has not been manipulated or modified by any intermediary sources or processes. The other options are not as important as taking the data directly from the system, as they do not affect the validity or reliability of the data. There is no privacy information in the data is a privacy concern that can help protect the confidentiality and integrity of personal or sensitive data, but it does not affect the accuracy or completeness of the data. The data can be obtained in a timely manner is a logistical concern that can help facilitate the efficiency and effectiveness of the data analytics process, but it does not affect the authenticity or accuracy of the data. The data analysis tools have been recently updated is a technical concern that can helpenhance the functionality and performance of the data analytics tools, but it does not affect the validity or reliability of the data. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 88

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

A. □□-□□□

B. □□□ □□(DoS)

C. SQL □□

D. □□□ □□□ □□□□

Answer: (SHOW ANSWER)

SQL injection attacks exploit vulnerabilities in web applications by inserting malicious SQL code into input fields, such as a search box. This can cause the server to execute unintended commands, often revealing restricted information.

* Man-in-the-Middle (Option A):This intercepts communication but does not involve code injection.
* Denial of Service (DoS) (Option B):This aims to disrupt service, not extract information.
* Cross-Site Scripting (Option D):Involves injecting malicious scripts to execute in a user's browser but does not extract server-side data.

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

NEW QUESTION: 89

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

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: 90
□□□□ □□□□□ □□ □□ □□□ □□□ □□□ □□ □□□ IT □ □□ □□□ □□ IS □□□□□ □□ □□ □□ □□□ □□□ □□□□.
A. □□□□□□□ □□□□□□□ □□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□□ □□□□□.
C. □□□□□ □□□□ □□□ □□□ □□□□□.
D. □□□□ □□ □□□ □□□ □□ □□
Answer: (SHOW ANSWER)
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: 91
□□ □□□□ □□□□ □□□□ □, □□ □ □□ □□□□ □ □□ □□ □□□ □□□□ □□ □□ □□□□□?
A. IS □□□□ □□ □□□ □□□ □□□□ □□□□.
B. □□□□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□□ □□□□ □□□□.
D. □□□□ □□ □□□□ □□□ □ □□□□.
Answer: B (LEAVE A REPLY)

The best situation that justifies the use of a smaller sample size when testing the accuracy of transaction data is B. It is expected that the population is error-free. The sample size is the number of items selected from the population for testing. The sample size depends on various factors, such as the level of confidence, the tolerable error rate, the expected error rate, and the variability of the population. A smaller sample size means that fewer items are tested, which reduces the cost and time of testing, but also increases the sampling risk (the risk that the sample is not representative of the population).
One of the factors that affects the sample size is the expected error rate, which is the auditor's best estimate of the proportion of errors in the population before testing. A higher expected error rate means that more errors are likely to be found in the population, which requires a larger sample size to provide sufficient evidence for the auditor's conclusion. A lower expected error rate means that fewer errors are likely to be found in the population, which allows a smaller sample size to provide sufficient evidence for the auditor's conclusion.
Therefore, if it is expected that the population is error-free (i.e., the expected error rate is zero or very low), a smaller sample size can be justified.
The other situations do not justify the use of a smaller sample size when testing the accuracy of transaction data. A. The IS audit staff has a high level of experience. The IS audit staff's level of experience does not affect the sample size, but rather their ability to design and execute the sampling procedures and evaluate the results. The IS audit staff's level of experience may affect their judgment in selecting and applying sampling methods, but it does not change the statistical or mathematical principles that determine the sample size. B.
Proper segregation of duties is in place. Proper segregation of duties is an internal control that helps prevent or detect errors or fraud in transaction processing, but it does not affect the sample size. The sample size is based on the characteristics of the population and the objectives of testing, not on the controls in place. Proper segregation of duties may reduce the likelihood or impact of errors or fraud in transaction processing, but it does not eliminate them completely. Therefore, proper segregation of duties does not justify a smaller sample size when testing the accuracy of transaction data. C. The data can be directly changed by users. The data's ability to be directly changed by users does not justify a smaller sample size, but rather a larger one. The data' s ability to be directly changed by users increases the risk of errors or fraud in transaction processing, which requires a larger sample size to provide sufficient evidence for the auditor's conclusion. The data's ability to be directly changed by users also increases the variability of the population, which affects the sample size.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* Audit Sampling - AICPA3

* How to choose a sample size (for the statistically challenged)

NEW QUESTION: 92
□□□ □□ □□ □ □□□ □□(SIEM) □□□□ □□□ □, □□ □ □□ □□□□ □□□ □□□□□?
A. SIEM □□□□ □□□ □□□□□.
B. SIEM □□□ □□ □□□□□.
C. SIEM□ □□□□ □□□□.
D. SIEM □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The greatest concern that the IS auditor should have when reviewing an organization's security information and event management (SIEM) solution is that the SIEM is decentralized. This is because a decentralized SIEM can pose challenges for collecting, correlating, analyzing and reporting on security events and incidents from multiple sources and locations. A decentralized SIEM can also increase the complexity and cost of maintaining and updating the SIEM components, as well as the risk of inconsistent or incomplete security monitoring and response. The IS auditor should recommend that the organization adopts a centralized or hybrid SIEM architecture that can provide a holistic and integrated view of the security posture and activities across the organization. The other findings are not as concerning as a decentralized SIEM, because they can be addressedby implementing best practices and standards for SIEM reporting and configuration. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.4

NEW QUESTION: 93
□□ □□□ □□□□ IS □□□□ □□□ □□□□ □□□.
A. □□□□□□ □□□□ □□ □□ □□□□□ □□□□ □□□□□.
B. □□□ □□□□□□ □□□□ □□ □□□ □□□□ □□□□□.
C. □□□□□□□ □□ □□ □□□ □□□ □□□□ □□□□□.
D. □□ □□□□ □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Upon completion of audit work, an IS auditor should distribute a summary of general findings to the members of the auditing team. This is to ensure that the audit team

members are aware of the audit results, have an opportunity to provide feedback, and can agree on the audit conclusions and recommendations.
Providing a report to senior management prior to discussion with the auditee, providing a report to the auditee stating the initial findings, and reviewing the working papers with the auditee are not appropriate actions for an IS auditor to take upon completion of audit work, as they may compromise the audit independence, objectivity, and quality. References: ISACA CISA Review Manual 27th Edition, page 221

NEW QUESTION: 94
IS □□□□ □□□ □□ □□ □□ □□□□□ □□□□ □□□□. □□ □ □□□□□ □ □ □ □□□□ □□□□□?
A. □ □□□□□□□ □□□ □□□ □□□ □□□ □□□ □□□□.
B. □□□□ □□□□ □□□□ □□□□□.
C. □□ □□□□□□ □□ □□□ □□□□ □□□□.
D. □□ □□ □□□ □ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
An IS auditor would be most concerned if process ownership has not been established for the information asset management process, as this would indicate a lack of accountability, responsibility, and authority for managing the assets throughout their lifecycle. The process owner should also ensure that the process is aligned with the organization's objectives, policies, and standards. The process should require specifying the physicallocations of assets, include asset review, and identify asset value, but these are less critical than establishing process ownership. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3

NEW QUESTION: 95
□□ □□ □□ □ □□□ □□□ □□□□ □□ □ □□□ □□□□ □□ □□□□□?
A. □□□□ □□□□ □□ □□□ □□□□.
B. □□□□ □□□□ □□□ □ □□□□.
C. □□□□ □□ □□ □□□ □□□□ □□□□.
D. □□ □□□ □□ 1□ □□ □□□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
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: 96
□□ □ □□□□□ □□ □□□□□ □□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□□□ □□ □□ □□□ □ □□□ □□ □□□□ □□ □□□□ □□□□□□□ □.
B. □□□ □□ □□□(UAT) □□ □□□ □□□ □□ □□ □□ □□□ □□□□□□□.
C. □□□ □□□□□ □□ □□□ □□ □□□□ □□□□□□□ □□□ □□□□□□□.
D. □□ □□□ □□ □□ □□□ □□□□ □□□□□ □□□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
□□ □ □□□□ □□□ □□ □□□(CASB)□ □□□ □□□□□ □□□□ □□□□ □□ □□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□□
B. □□ CASB □□ □□
C. □□□□□□ □□
D. □□□ □□□ □□
Answer: (SHOW ANSWER)
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 aninneffective 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: 98
□□□ □ □□□□□□□ □□□ □ □□□ □□□ □□□□ □ □□ □ □□ □□ □□□ □□ □□□□□□?
A. □□□ □□ □□

B. □□□ □□□
C. □□ □□□ □□(BCP)
D. □□ □□□□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Thoroughsystem testingbefore deployment helps identify potentialbugs, vulnerabilities, and performance issuesto prevent system failures.
* System Testing (Correct Answer - B)
* Detects defects that could lead to system crashes.
* Ensures compatibility and performance stability.
* Example:Stress testing an e-commerce application to prevent crashes on Black Friday.
* System Recovery Plan (Incorrect - A)
* Focuses on recovery after failure rather than prevention.
* Business Continuity Plan (Incorrect - C)
* Addresses overall business resilience, not application stability.
* Transaction Monitoring (Incorrect - D)
* Detects fraud and anomalies but does not prevent failures.
References:
* ISACA CISA Review Manual
* NIST 800-160 (Systems Security Engineering)

NEW QUESTION: 99
□□ □ □□□□ □□□ □□(BCP)□ □□ □□□ □□□□□ □□□□ □□□ □□ □□ □ □□□□ □□ □□□□□?
A. □□□□ □□□ □□
B. □□□□ □□□ □□
C. □□□□□ □□□ □□
D. □□ □□ □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
□□ □ □□□ □□ □□(DLP) □□□ □□□□ □ □□ □□ □□□ □□ □□□ □□□□ □?
A. □□□□ □□ □□□ □□□□ □□ □□□ □□□□ □□ □□
B. □□□ □□□ □□□ □□□□□□ □□ □□ □ □□ □□ □□ □□ □ □□
C. □□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□□
D. □□ □□□ □□□ □ □□ □□□□□ □□ □□ □□□ □□ □□ □□
Answer: B (LEAVE A REPLY)
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: 101
□□□ □□ □□□ □□□ □, IS □□□□ □□ □□□□ □□□□ □ □□□ □□□ □□ □□.
A. □ □□ □□□ □□ □□ □□□ □□□□□.
B. □□ □□□ □ □□□ □□ □□□□ □□□□□ □□□□.
C. □□ IT □□□□ □□ □□□□ □□□□□.
D. □□ □□□□ □□□ □□ □□□□ □□□□ □□□.
Answer: B (LEAVE A REPLY)
When reviewing a data classification scheme, it is most important for an IS auditor to determine if the security criteria are clearly documented for each classification. This will help the IS auditor to evaluate if the data classification scheme is consistent, comprehensive, and aligned with the organizational objectives and regulatory requirements. The security criteria should define the level of confidentiality,integrity, and availability for each data classification, aswell as the corresponding controls such as access control, rights management, and cryptographic protection1. The other options are less important or incorrect because:
* A. Each information asset is not necessarily assigned to a different classification. Data classification schemesusually have a limited number of categories, such as "Sensitive," "Confidential," and "Public," and multiple information assets can belong to the same category2.
* C. Senior IT managers are not necessarily identified as information owners. Information owners are typically the business units or functions that create, use, or maintain the information assets, and they may or may not be senior IT managers3.
* D. The information owner is not required to approve access to the asset. The information owner is responsible for defining the access requirements and rules for the asset, but the actual approval of access requests may be delegated to other roles, such as data custodians or administrators3. References: Simplify and Contextualize Your Data Classification Efforts - ISACA, 3.7: Establish and Maintain a Data Classification Scheme, Data Classification and Practices - NIST, CISA Exam Content Outline |CISA Certification | ISACA

NEW QUESTION: 102
□□□□ □□□□ □□ □□□ □□□ □□□ □□□□□ □□□□□. □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□ □□□□?
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: 103

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

A. □□□□□ □□ □□ □□□□ □□□□□□□.

B. □□ □□ □□(KPI)□ □ □ □ □□ □□□□□□□.

C. □□□ □□ □□□□□ □□□□ □□□□.

D. □□ □□□ □□ □□□ □□ □□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 104

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

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: 105
□□ □□□ □□ □□□ □□(EDI) □□□□ □□ □□□ □□ □□□□ □□□ □□□ □ □□□ □□□□.
A. □□□,
B. □□□.
C. □□ □□,
D. □□ □□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
IS □□□□ RPA(□□ □□□□ □□□) □□□ □□□ □ □□ □ □□ □□ □□□ □□ □□□?
A. □□ □□□ □□□□□ □□□□□.
B. □□□ □□□□ □□ □□□ □□□□□.
C. □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□ □□□ □□□□□.
D. □□□ □□□□□ □□□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
□□ □ IS □□ □□□□ □□□□ □□□□ □□ □□ IS □□□ □□□ □□□ □□□□ □□ □□□ □□□□□?
A. □□□ □□□□ □□□□□ □□
B. □□ □□ □□ □□□ □□□ □□□ □□□□□□ □□□□ □□

C. □□□ □□□ □□□□□ □□□□□□ □□□□ □□
D. □□□ □□ □□□ □□ □□□□□ □□□□ □□
Answer: (SHOW ANSWER)
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: 108
□□ □□ □□□ □□ □□□ □□□ □□□□.
A. □□ □□□ □□□□□.
B. □□□ □□□ □□□ □ □□□ □□□.
C. □□ □□□□ □□□ □ □□□ □□□.
D. □□ □□ □□□ □□ □ □□□□.
Answer: D (LEAVE A REPLY)
The primary benefit of information asset classification is that it enables risk management decisions.
Information asset classification helps to identify the value, sensitivity and criticality of information assets, and to determine the appropriate level of protection and controls required for them. This facilitates risk assessment and risk treatment processes, and ensures that information assets are aligned with business objectives and regulatory requirements. Preventing loss of assets, helping to align organizational objectives or facilitating budgeting accuracy are secondary benefits of information asset classification, but not the main purpose. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 300

NEW QUESTION: 109
□□ □ □□ □□ □□□ □□□ □□□ □□ □□ □□ □□□ □□□□□ □□ □□ □□ □□ □□□ □□□□□?

A. □□□□/PIN □□
B. □□ □□ □□□□□
C. □□ □□□
D. □□□ □□
Answer: (SHOW ANSWER)
The best control to minimize the risk of unauthorized access to lost company-owned mobile devices is device encryption. Device encryption is a process that transforms data on a device into an unreadable format using a cryptographic key. Device encryption protects the data stored on the device from being accessed by unauthorized parties, even if they bypass the password or PIN protection. Device encryption can also prevent data leakage if the device is disposed of or recycled without proper data sanitization. Password or PIN protection is a basic control that prevents unauthorized access to the device by requiring a secret code or pattern to unlock it. However, password or PIN protection can be easily compromised by brute force attacks, shoulder surfing, or social engineering. Device tracking software is a tool that allows the device owner or administrator to locate, lock, or wipe the device remotely in case of loss or theft. However, device tracking software depends on the device's network connectivity and GPS functionality, which may not be available or reliable in some situations. Periodic backup is a process that copies the data from the device to another storage location for recovery purposes. Periodic backup can help restore the data in case of loss or damage of the device, but it does not prevent unauthorized access to the data on the device itself. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.4: Mobile Devices

NEW QUESTION: 110
IS □□□□ □□□□□□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□. □□ □□ □□□ □□ □□□□ □□□□ □□□ □□□□□ □□□. □□ □□□ □□□ □□ □□□?
A. □□□□□ □□□
B. □□□ □□□
C. □□ □□□
D. □□□ □□□
Answer: (SHOW ANSWER)
Discovery sampling is an appropriate sampling method for an IS auditor who intends to launch an intensive investigation if one exception is found. Discovery sampling is a type of attribute sampling that determines the sample size based on an acceptable risk of not finding at least one occurrence of an attribute when a given rate of occurrence exists in a population. Discovery sampling can be used by an IS auditor who wants to detect fraud or errors that have a low probability but high impact on an audit objective. The other options are not appropriate sampling methods for this purpose, as they may involve judgmental sampling, variable sampling, or stratified sampling. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.31

* CISA Review Questions, Answers & Explanations Database, Question ID 230

NEW QUESTION: 111
□□ □□□ □□□ □□□ □□ □□□□□ □□□ □□□□ □□ 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: 112
□□ □□ □□ □□ IS □□□□ □□□□ □□ □□(BIA)□ □□□□ □□□□ □□ □□ □□□. □□□□ □□ □□□ □□□□ □□□.
A. □□ □□ □□(BIA)□ □□□□□.
B. □□□□□ □□ □□□□ □□□□□.
C. □□ □□ □□ □□□ □□□ □□□ □□□□□.
D. □□□□ □□ □□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
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: 113
□□ □ □□ □□ □□□ □□ □□ □□ □□□ □□□ □□ □□□ □□□□ □ □□ □□ □□□?
A. □□□ □□ □□□□ □□ □□□□ □□ □□
B. □□□□ □□□□□ □□ □□□□ □□ □□ □□□□□ □□
C. □□□ □□ □□ □□□□ □□□□ □□□ ID□ □□□ □□□□□.
D. □□□ □□ □□ □□□ □□□□□ □□
Answer: D (LEAVE A REPLY)
Segregation of duties (SoD) is a key internal control that aims to prevent fraud and errors by ensuring that no single individual can perform incompatible or conflicting tasks within a business process. SoD reduces the risk of unauthorized or improper transactions, manipulation of data, or misappropriation of assets.
In the accounts payable department, SoD involves separating the following functions: invoice processing, payment authorization, payment execution, and reconciliation. For example, the person who approves an invoice should not be the same person who issues the payment or reconciles the bank statement.
One of the best ways to ensure appropriate SoD within the accounts payable department is to restrict program functionality according to user security profiles. This means that each user of the accounts payable system should have a unique login and password, and should only have access to the functions that are relevant to their role and responsibilities. For instance, an invoice processor should not be able to approve payments or modify vendor records. This way, the system can enforce SoD and prevent unauthorized or fraudulent activities.
The other options are not as effective as restricting program functionality according to user security profiles.
Restricting access to update programs to accounts payable staff only is a general access control measure, but it does not address the SoD issue within the accounts payable department. Including the creator's user ID as a field in every transaction record created is a useful audit trail feature, but it does not prevent users from performing incompatible functions. Ensuring that audit trails exist for transactions is a detective control that can help

identify and investigate any irregularities, but it does not prevent them from occurring in the first place.

NEW QUESTION: 114
□□ □ □□□ □□ □□□□□ □□ □□ □□□□□ □□□□ □ □□ □□□ □□ □□ □□□?
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: 115
□□□□□ □□□ □□□ □□□□□□ □□□ □□ □ □□ □□□ □□ □□□□□?
A. □ □□□□□□ □□□ □□□ □□□ □□□□.
B. □□□□ □□ □□□ □ □□□□□□□.

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

NEW QUESTION: 116
□□□ □□□□ □□□□ □□□□□ □□□□ □□□ □□□□ □□□.
A. □□□ □□ □□□□ □□□□ □□ □□ □□□ □□□ □□ □□□□□ □□□□□.
B. □□□ □□ □□□□ □□□□ □□ □□ □□□ □□ □□□□□ □□ □□ □□□□ □ □□□□□.
C. □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□□□□ □□□□□.
D. □□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□□□ □□ □□ □□□□ □ □□□□□.
Answer: A (LEAVE A REPLY)
To confirm integrity for a hashed message, the receiver should use the same hashing algorithm as the sender' s to create a binary image of the file. A hashing algorithm is a mathematical function that transforms an input data into a fixed-length output value, called a hash or a digest. A hashing algorithm has two main properties:
it is one-way, meaning that it is easy to compute the hash from the input, but hard to recover the input from the hash; and it is collision-resistant, meaning that it is very unlikely to find two different inputs that produce the same hash. These properties make hashing algorithms useful for verifying the integrity of data, as any change in the input data will result in a different hash value. Therefore, to confirm integrity for a hashed message, the receiver should use the same hashing algorithm as the sender's to create a binary image of the file, which is a representation of the file in bits (0s and 1s). The receiver should then compare this binary image with the hash value sent by the sender. If they match, then the message has not been altered in transit.
If they do not match, then the message has been corrupted or tampered with.
References:
* Ensuring Data Integrity with Hash Codes
* Message Integrity

NEW QUESTION: 117
□□ □ □□□ □□□□□ □□□□ □□□ □□□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□ □□
B. □□
C. □□□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
The best way to ensure data integrity across system interfaces is to perform reconciliation. Reconciliation is the process of comparing and verifying the data from different sources or

systems to ensure that they are consistent, accurate, and complete. Reconciliation can help to identify and resolve any discrepancies, errors, or anomalies in the data that could affect the quality, reliability, or validity of the information. Reconciliation can also help to detect and prevent any unauthorized or fraudulent data manipulation or modification.
References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 118
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: 119
IS □□□□ □□□ □□□□ □□ □□ □□ □□□ □□□ □□□□ □□ □□ □□□□ □□. □ □□□□ □□□ □□ □ □□□ □□ □ □□ □□□□?
A. □□□□□ □□□□ □□□□ □□ □ □□□□.
B. □□□□ □□□ □□ □□□ □□□□ □□ □ □□□□.
C. □□□ □□ □□□□ □□□□ □□ □ □□□□.
D. □□ □□□□ □□□□ □□ □ □□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
□□□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□□ □□
B. □□□□ □□□□□ □□ □□ □□□□ □□□□.
C. □□ □ □□□□ □□□□ □□ □□□ □□□ □□□□.
D. □□ □□ □□ □ □□ □□□□□ □□□□.
Answer: C (LEAVE A REPLY)
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: 121
IS □□□□ □□□ □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□. □□ □□□ □ □□ □□□ □ □□ □□□ □□□□ □□ □□□□□?
A. □□□ □□□
B. □□□ □□ □□□
C. □□ □□□
D. □□ □□ □□□

Answer: (SHOW ANSWER)
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: 122
□□□□□ IT □□□ □□□□ □□ □□□ □□□ □□□ □, □□□ □□□□ IT □□ □ □□□ □□□□ □ □□ □□□ □□ □□□ □□ □ □□ □□□□?
A. □□□□ IT □□ □□□ □□□□□□.
B. □□□□ □ □□ □□ □□□ □□ IT □□ □□□ □□□□□.
C. □□□ IT □□ □□□□□ □□ □□ □□
D. □□□ IT □□ □□ □□ □□
Answer: C (LEAVE A REPLY)
The best approach for determining the overall IT risk appetite of an organization when business units use different methods for managing IT risks is to prioritize the organization's IT risk scenarios. IT risk appetite is the amount and type of IT risk that an organization is willing to accept in pursuit of its objectives. IT risk scenarios are hypothetical situations that describe the potential impact of IT risk events on the organization's objectives, processes, and resources. By prioritizing the organization's IT risk scenarios, the IS auditor can identify the most significant IT risks that affect the organization as a whole, and align them with the organization's strategic goals, values, and culture. Prioritizing the organization's IT risk scenarios can also help to communicate and monitor the IT risk appetite across the organization, and facilitate consistent and informed decision making. The other approaches (A, B and D) are not effective for determining the overall IT risk appetite of an organization, as they do not consider the impact and likelihood of IT risks on the organization's objectives, nor do they account for the diversity and complexity of IT risks

across different business units. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of Information Technology, Section 2.3: Information Technology Risk Management

NEW QUESTION: 123
□□ □□ □□(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: 124
□□□ □□ □□□ □□ □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □ □□□. □□ □ □□ □□□ □ □□□ □□□□ □ □□ □□□□□?
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: 125
□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□□□□ □□□□ □□□□.
□ □□□□ □□ □□□ □ □□ □□ □ □□□ □□ □ □□ □□□□?
A. □□ □□ □□□ □□ □□□ □□
B. □□ □□ □□
C. □□□ □□ □□ □□□
D. □□□ □□□ □□
Answer: (SHOW ANSWER)
An acceptable use policy (AUP) is a document that defines the rules and guidelines for using an organization' s IT resources, such as networks, devices, and software. It aims to protect the organization's assets, security, and productivity. An AUP should be formally acknowledged by users to ensure that they are aware of their responsibilities and obligations when using the IT resources. Without formal acknowledgment, users may not be held accountable for violating the AUP or may claim ignorance of the policy. This can expose the organization to legal, regulatory, reputational, or operational risks. Lack of data for measuring compliance, violation of industry standards, and noncompliance with documentation requirements are also possible risks from not having users acknowledge the AUP, but they are less significant than lack of user accountability. References: Workable: Acceptable use policy template, Wikipedia: Acceptable use policy

NEW QUESTION: 126
□□ □□□ □□□□ □□ □□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □ □□ □□□. □□ □ 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: 127
□□ □ IS □□□□ □□□ □□ □□□ □□ □□□□□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□ □□
B. □□□□□□ □□

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

NEW QUESTION: 128
□□ □ □□□ □□ □□(QC) □□□□ □□ □□□ □□ □ □□□ □□□□ □□ □□□ □□?
A. □□ □□ □□
B. □□ QC □□ □□
C. □□ □ □□ □□
D. □□ □□ □ □□□ □□
Answer: C (LEAVE A REPLY)
The greatest risk to an organization's ability to manage QC processes is the lack of policies and procedures that define the QC objectives, standards, methods, roles, and responsibilities. Without policies and procedures, the QC processes may be inconsistent, ineffective, inefficient, or noncompliant with the relevant regulations and best practices. Policies and procedures provide the foundation and guidance for the QC processes and help to ensure their quality, reliability, and accountability.
References
ISACA CISA Review Manual, 27th Edition, page 253
Quality Control - an overview | ScienceDirect Topics
Quality Control: Meaning, Importance, Definition and Objectives

NEW QUESTION: 129
□□□ □□ □□ □□□□□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □ □□□□?
A. □□□□□□□ □□ 2□□ □□□□□□ □□□□□.
B. □□ □□□□ □□ □□ □□ □□□ □□□□ □□□□□.
C. □□ □□ □□□ □□ □□ □□ □□□ □□□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)
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: 130
□□□□ □□ □□ □□(CSA) □□□□□ □□ □□□ □□ □□□□□?
A. □□ □□ □□
B. □□ □□□ □□ □□
C. □□ □□□ □□ □□
D. □□□□ □□□□ □□
Answer: D (LEAVE A REPLY)
Understanding the business process is the most important factor for an effective control self-assessment (CSA) program. A CSA program 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. A CSA program can help identify risks and potential exposures to achieving strategic business objectives, evaluate the adequacy and effectiveness ofcontrols, and implement remediation plans to address any gaps or weaknesses2. To conduct a successful CSA, it is essential to have a clear and comprehensive understanding of the business process under review, including its objectives, inputs, outputs, activities, resources, dependencies, stakeholders, performance indicators, etc. This will help to identify the relevant risks and controls associated with the process, as well as to evaluate their impact and likelihood. Determining the scope of the assessment, performing detailed test procedures, and evaluating changes to the risk environment are also important factors for an effective CSA program, but not as important as understanding the business process. These factors are more related to the execution and monitoring phases of the CSA program, while understanding the business process is related to the planning and preparation phase. Without a solid understanding of the business process, the scope, testing, and evaluation of the CSA may not be accurate or complete. References: ISACA CISA Review Manual 27th Edition, page 310

NEW QUESTION: 131
□□□□ □□□ □□ □□(DLP) □□□□ □□□□ □□ □□ □ □□ □□ □□□□ □□ □□□ □□□□□?
A. □□□ □□
B. □□ □□ □□
C. □□ □□□ □□□
D. □□ □□□□ □□
Answer: B (LEAVE A REPLY)
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: 132
□□□ □□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□□ □□□□ □□□ □□□.
A. □□ □□□.
B. □□,
C. □□□.
D. □□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 133
IS □□□□ □□□□ □□ □□□□ □□ □□□ □ □□ □□□□□□□ □□□ □□□□ □. □ □□□ □□□□□□ □□□ □□□□ □ □□□□□ □□ □□□□ □□□□. □□ □□ □□ □□ □□□ □□□□ □□□□□. IS □□□□ □ □□ □□□ □□□ □□□ □ □□.
A. □□□□□□□ □□ □□□□ □□□ □□ □□□ □□ □□□□□.
B. □□□□□□ □□□□ □ □□□ □□□□□ □□□□ □□□□□.
C. □□□□ □□ □□□ □□□□□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The IS auditor's first action after discovering an option in a database that allows the administrator to directly modify any table should be to determine whether the audit trail is secured and reviewed. This is because direct modification of database tables can pose a significant risk to data integrity, security, and accountability. An audit trail is a record of all changes made to database tables, including who made them, when they were made, and what was changed. An audit trail can help to detect unauthorized or erroneous changes, provide evidence for investigations or audits, and support data recovery or restoration. The IS auditor should assess whether the audit trail is protected from tampering or deletion, and whether it is regularly reviewed for anomalies or exceptions.

NEW QUESTION: 134
□□ □□ □□ □□ □□ □□□ □□ □□□□ □□ □□ □□ □□□□□?

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: 135
□□□ □□ □□ □□□ □□□□ □□□ □ IS □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. IT □□□□□ □□□
B. □□ □□
C. IT □□ □□□□ □□
D. □□ □□ □□ □□
Answer: B (LEAVE A REPLY)
The most important consideration for an IS auditor when assessing the adequacy of an organization's information security policy is the business objectives. An information security policy is a document that defines the organization's approach to protecting its information assets from internal and external threats. It should align with the organization's mission, vision, values, and goals, and support its business processes and functions1. An informationsecurity policy should also be focused on the business needs and requirements of the organization, rather than on technical details orspecific solutions2.
The other options are not as important as the business objectives, because they do not directly reflect the organization's purpose and direction. IT steering committee minutes are records of the discussions and decisions made by a group of senior executives who oversee the IT strategy and governance of the organization. They may provide some insights into the information security policy, but they are not sufficientto evaluate its adequacy3. Alignment with the IT tactical plan is a measure of how well the information security policy supports the short-term actions and projects that implement the IT strategy.

However, the IT tactical plan itself shouldbe aligned with the business objectives, and not vice versa4. Compliance with industry best practice is a desirable quality of an information security policy, but it is not a guarantee of its effectiveness or suitability for the organization. Industry best practices are general guidelines or recommendations that may not apply to every organization or situation. An information security policy should be customized and tailored to the specific context and needs of the organization. References:
* The 12 Elements of an Information Security Policy | Exabeam1
* 11 Key Elements of an Information Security Policy | Egnyte2
* What is an IT steering committee? Definition, roles & responsibilities ...3
* What is IT Strategy? Definition, Components & Best Practices | BMC ...4
* IT Security Policy: Key Components & Best Practices for Every Business

NEW QUESTION: 136
□□□□ □□□□ □□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□ □□□□ □□ □□ □ □□□ □□□□□□. □□ □ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□ □□□
B. □□ □□□□□ □ □□
C. □□ □□□ □□
D. □□□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 137
□□□□□ □□ □□□ □□□□□ □□□ □□ □□□ □□□ □□ □□□□ □□□□ □ □ □□□ □□□ □□ □ □□□□□. □□ □□□ □□ □□□□ □□□ □□□ □□□ □ □ □ □□□ □ □□□□□?
A. □□□□□ □□ □□ □□
B. □□ □□□ □□□ □□□
C. □□□ □□ □□□ □□ □□□□ □□ □□
D. □□ □□□ □□□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
Separate authorization for input of transactions. This control would have best prevented this type of fraud in a retail environment by ensuring that the warehouse employee who handles the inventory items does not have the authority to enter adjustments to the

inventory system. This would create a segregation of duties that would reduce the risk of collusion and concealment of theft.
The other options are not as effective as option A in preventing this type of fraud. Option B, statistical sampling of adjustment transactions, is a detective control that may help identify fraudulent transactions after they have occurred, but it does not prevent them from happening in the first place. Option C, unscheduled audits of lost stock lines, is also a detective control that may reveal discrepancies between the physical and recorded inventory, but it does not address the root cause of the fraud. Option D, an edit check for the validity of the inventory transaction, is a preventive control that may help verify the accuracy and completeness of the transaction data, but it does not prevent unauthorized or fraudulent adjustments.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription
* Different Types of Inventory Fraud and How to Prevent Them1
* 6 Ways to Prevent Inventory Fraud in Your Business2

NEW QUESTION: 138
□□ □□□□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□ 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: 139
□□ □ □□ □□ □□(DRP)□ □□□ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□□.
B. □□□ □□□□ □□□□ □□ □□□□□.
C. □□□□ □□□ □□ □□□ □□□□□.
D. □□□□ □□□ □ □□ □□□ □□ □□□ □□□□.
Answer: (SHOW ANSWER)
The most important reason to classify a disaster recovery plan (DRP) as confidential is to reduce the risk of data leakage that could lead to an attack. A DRP contains sensitive information about the organization's IT infrastructure, systems, processes, and procedures for recovering from a disaster. If this information falls into the wrong hands, it could be exploited by malicious actors to launch targeted attacks, sabotage recovery efforts, or extort ransom. Therefore, a DRP should be protected from unauthorized access, disclosure, modification, or destruction.
The other options are not as important as reducing the risk of data leakage that could lead to an attack:
* Ensuring compliance with the data classification policy is a good practice, but it is not a sufficient reason to classify a DRP as confidential. The data classification policy should reflect the level of risk and impact associated with each type of data, and a DRP should be classified as confidential based on its potential harm if compromised.
* Protecting the plan from unauthorized alteration is a valid concern, but it is not a primary reason to classify a DRP as confidential. A DRP should be protected from unauthorized alteration by implementing access controls, audit trails, version control, and change management processes.
Classifying a DRP as confidential may deter some unauthorized alterations, but it does not prevent them.
* Complying with business continuity best practice is a desirable goal, but it is not a compelling reason to classify a DRP as confidential. Business continuity best practice may recommend classifying a DRP as confidential, but it does not mandate it. The decision to

classify a DRP as confidential should be based on a risk assessment and a cost-benefit analysis.

NEW QUESTION: 140
□□□ □□□ □□□□ □□ □□□ BYOD(Bring Your Own Device) □□□ □□□□ □ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□□ BYOD □□□ □□□□ □□□ □□□□ □□ □□□ □□□□□ □□□□ □.
B. BYOD □□□□ □□ □□ □□□ □□□□□.
C. □□ □□ □□□ BYOD □□□ □□□□ □□□ □□□ □□□□□.
D. □□□ BYOD □□□ □□□□□ □□□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The best recommendation to include in an organization's bring your own device (BYOD) policy to help prevent data leakage is to require multi-factor authentication on BYOD devices. BYOD is a practice that allows employees to use their own personal devices, such as smartphones, tablets, or laptops, to access the organization's network, data, and systems. Data leakage is a risk that involves the unauthorized or accidental disclosure or transfer of sensitive or confidential data from the organization to external parties or devices.
Multi-factor authentication is a security measure that requires users to provide two or more pieces of evidence to verify their identity and access rights, such as passwords, tokens, biometrics, or codes. Multi-factor authentication can help prevent data leakage by reducing the likelihood of unauthorized access to the organization's data and systems through BYOD devices, especially if they are lost, stolen, or compromised. The other options are not as effective as requiring multi-factor authentication on BYOD devices, because they either do not prevent data leakage directly, or they are reactive rather than proactive measures. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

NEW QUESTION: 141
□□ □□□ □□ □□ □□ □ □□ □□ □□□□ □□□ □□ □□ □□□ □□□□ □ □ □ □□□ □□□?
A. □□ □□ □□(CSA)
B. □□ □□
C. □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 142
□□□ □□□ □□□ □□□ □□□□ □□□, □□□ □□ □□ □□□ □□□ □□□□ □.
□□ □ □□ □□□ □□ □□□□ □□ □□ □□□□□?

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

NEW QUESTION: 143
□□ □□□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□, □□ □□□□ □□□ □□□□□ □□ □ □□ □□□ □□□□□□ □□ □□□□. □□ □ □□ □□□□ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□□□ □□□□□ □□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□□□
D. □□□ □□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
The senior auditor's most appropriate course of action is to have the finding reinstated, because the auditee's claim of correcting the problem is not sufficient evidence to support the removal of the finding. The auditor should verify that the corrective action has been implemented effectively and that it has resolved the underlying issue or risk. The auditor should also document the evidence and results of the verification in the work papers. The other options are not appropriate, because they either accept the auditee's claim without verification, delegate the responsibility to the auditee or escalate the issue unnecessarily.
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: 144
□□ □ □ □□□ □□ □□□□ □□□□ □ □□ □□ □ □□□ □□□□□?
A. □□□ □□□
B. □□□ □□□
C. □□□ □□□
D. □□□ □□□
Answer: (SHOW ANSWER)
The greatest risk associated with storing customer data on a web server is data confidentiality. Data confidentiality is the property that ensures that data are accessible only to authorized entities or individuals, and protected from unauthorized disclosure or exposure. Storing customer data on a web server poses a high risk to data confidentiality, as web servers are exposed to the internet and may be vulnerable to various types of attacks or breaches that can compromise the security and privacy of customer data, such as hacking, phishing, malware, denial of service (DoS), etc. Customer data may contain

sensitive or personal information that can cause harm or damage to customers or the organization if disclosed or exposed, such as identity theft, fraud, reputation loss, legal liability, etc. Data availability is the property that ensures that data are accessible and usable by authorized entities or individuals when needed. Data availability is a risk associated with storing customer data on a web server, as web servers may experience failures or disruptions that can affect the accessibility and usability of customer data, such as hardware faults, network issues, power outages, etc.
However, data availability is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data integrity is the property that ensures that data are accurate and consistent, and protected from unauthorized modification or corruption. Data integrity is a risk associated with storing customer data on a web server, as web servers may be subject to attacks or errors that can affect the accuracy and consistency of customer data, such as injection attacks, tampering, replication issues, etc. However, data integrity is not the greatest risk associated with storing customer data on a web server, as it does not affect the security and privacy of customer data. Data redundancy is the condition of having duplicate or unnecessary data in a database or system. Data redundancy is not a risk associated with storing customer data on a web server, but rather a result of poor database design or management.

NEW QUESTION: 145
□□ □ IT □□□□ □□ □□□□ □□□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□□□□ □□□□ □□□ □□□□ □□
B. □□ □□ □□ □□□□□ □□ □□ □□
C. IT □□□ □□ □ □□
D. □□□□ □□ □□ □□ □□
Answer: A (LEAVE A REPLY)
Effective governance over IT infrastructure is indicated by the ability to deliver continuous, reliable performance12. This is because good governance ensures that IT investments support business objectives and produce measurable results towards achieving their strategies2. It involves implementing management and internal controls, strengthening security, financial controls, risk mitigation, and inspection and compliance obligations3. While security awareness programs, the number of servers, and the number of security incidents can be aspects of IT governance, they are not the best indicators of its effectiveness.
References:
The Value of IT Governance - ISACA
What is IT governance? A formal way to align IT & business strategy | CIO Robust Governance - KPMG Global

NEW QUESTION: 146

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

A. □□□ □□ □□□□ □□□ □□□ □□□□□.

B. □□, □□, □□(ETL) □□□ □□ □□□□ □□□□□.

C. □□ □□□□ □□□□□□□□ □□□ □□ □□□ □□□□□.

D. □□□ □□ □□ □□□□□□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

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: 147

□□□□□ RFID□ □□□ □ IS □□□□ □□ □□□□ □ □□ □□□□□?

A. □□□□□□

B. □□□□□

C. □□□

D. □□ □□

Answer: A (LEAVE A REPLY)

RFID stands for Radio Frequency Identification, and it is a technology that uses radio waves to identify or track objects that have a small chip (RFID tag) attached to them. RFID tags can store various types of information, such as serial numbers, product codes, or personal data. RFID readers can scan the tags from a distance and access the information without physical contact1.

RFID has many benefits for different applications, such as inventory management, supply chain optimization, asset tracking, and access control. However, RFID also poses some challenges and risks for information security and privacy. Some of these risks are:

Privacy: RFID tags can be read by unauthorized or malicious parties, who can collect personal or sensitive data without the knowledge or consent of the tag owners. This can lead to identity theft, profiling, tracking, or surveillance2. For example, a hacker could scan

an RFID-tagged passport or credit card and steal the personal information or financial details of the owner3.
Communication attacks: RFID systems are vulnerable to various types of attacks that target the wireless communication between the tags and the readers. These include eavesdropping, jamming, spoofing, replaying, cloning, or modifying the data transmitted by the tags or the readers4. For example, an attacker could intercept the data from an RFID tag and alter it before sending it to the reader, causing false or misleading information to be recorded.
Mafia fraud: This is a type of attack where an adversary acts as a man-in-the-middle and relays the information between two legitimate parties. This can allow the adversary to bypass authentication or authorization mechanisms and gain access to restricted areas or resources. For example, an attacker could use a device to relay the signal from an RFID-tagged car key to the car's ignition system and start the car without having the physical key.

NEW QUESTION: 148
□□ □ IS □□□□ □□ □□ □□□□ □□□ □□□ □□□ □ □□ □□□ □□ □□□ □□?
A. □□□□ □□□□ □□□□ □□ □ □□
B. □□□ □□□ □□□□ □□, □□ □ □□□ □□ □□□ □□ □□
C. □□ □□□□ □□□ □□□□ □□□□ □□ □□□ □□ □□ □□□
D. □□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□□
Answer: B (LEAVE A REPLY)
The answer B is correct because a system-generated list of staff and their project assignments, roles, and responsibilities is the most useful to an IS auditor performing a review of access controls for a document management system. A document management system is a software that helps organizations store, manage, and share documents electronically. Access controls are the mechanisms that restrict or allow access to the documents based on predefined criteria, such as user identity, role, or project. An IS auditor needs to verify that the access controls are properly configured and implemented to ensure the security, confidentiality, and integrity of the documents.
A system-generated list of staff and their project assignments, roles, and responsibilities can help the IS auditor to perform the following tasks:
* Identify the users who have access to the document management system and their level of access (e.g., read-only, edit, delete, etc.).
* Compare the actual access rights of the users with their expected or authorized access rights based on their roles and responsibilities.
* Detect any anomalies, discrepancies, or violations in the access rights of the users, such as excessive or unauthorized access, segregation of duties conflicts, or dormant or inactive accounts.

* Evaluate the effectiveness and efficiency of the access control policies and procedures, such as user provisioning, deprovisioning, authentication, authorization, auditing, etc.
The other options are not as useful as option B. Policies and procedures for managing documents provided by department heads (option A) are not reliable sources of information for an IS auditor because they may not reflect the actual practices or compliance status of the document management system. Previous audit reports related to other departments' use of the same system (option C) are not relevant for an IS auditor because they may not address the specific issues or risks associatedwith the current department's use of the document management system. Information provided by the audit team lead on the authentication systems used by the department (option D) is not sufficient for an IS auditor because authentication is only one aspect of access control and it does not provide information on the authorization or auditing of the document access.
References:
* Overview of document management in SharePoint
* Setting Up a Document Control System: 6 Basic Steps
* Access Control Management: Purpose, Types,Tools, & Benefits
* 9 Best Document Management Systems of 2023

NEW QUESTION: 149
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: 150
□□□ □□ □□□□ □□ □□□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□□□. □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□□□ □□□ □□ □□ □□ □□□ □□□□ □□□□.
B. □□ □□□ □□ □□ □□ □□ □□□ □ □□□ □□□.
C. □ □□ □□□ □□ □□□ □□□ □□□ □□□□.
D. □□ □□□ □□□ □□□□ □□□ □□ □□□□□.
Answer: D (LEAVE A REPLY)
The most important thing for the organization to ensure when reducing the actual retention period for media containing completed low-value transactions is that the retention period complies with data owner responsibilities. Data owners are accountable for the quality, security, and availability of the data under their control. They are also responsible for defining and enforcing data retention policies that comply with legal, regulatory, contractual, and business requirements. Data owners should be consulted and involved in any decision that affects the retention period of their data, as they are ultimately liable for any consequences of data loss or breach.
The policy includes a strong risk-based approach, the retention period allows for review during the year-end audit, and the total transaction amount has no impact on financial reporting are not the most important things for the organization to ensure when reducing the actual retention period for media containing completed low- value transactions. These are possible factors or benefits that may influence or justify the decision, but they do not override or replace the data owner responsibilities.

NEW QUESTION: 151
□□ □ □□ □□□□ □□□□ □□□□□ □□ □□□ □□ □□□ □□□□ □□□ □ □□ □□ 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: 152
□□□ □□□□□□ □□□□(EA)□ □□□ □, IS □□□□ EA □□□□ □□ □□ □□ □ □□ □□□ □□□□□?
A. IT □□ □ □□ □□□□ □□ □□□ □□
B. □□□ □□□ □□
C. □□ □□□□ □□ □□□□ □□□ □□□□ □□□
D. □□□ □ □□□ □□□□ □□□□
Answer: C (LEAVE A REPLY)
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: 153
□□ □□□□ □□□ □□□□ IS □□□□ □□ □ □□□ □□□ □□□□□□□. □□ □ □□□ □□ □ □□□ □□ □□□□ □□ □□ □□□□□?
A. □□□ □□□ □□□ □□ □ □□□ □□ □□□ □□□□ □□□□.
B. □□ □□□ □□□□ □□ □□ □□ □□□□□□.
C. □□□□ □□□ IT □□□□ □□□□□ □□□ □□□ □□□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□□□□□ □□□□.
Answer: D (LEAVE A REPLY)
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: 154
IS □□□□ □□ □□□ □□□ □□□□ □□□ □ □□□□ □□□□□ 95% □□□ □ □ □□□□□□.
□□ □ IS □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□
B. □□□ □□(DoS) □□
C. □□□
D. □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 155

CFO□ □□ □□ □□ □ □□□ □□ □□□ □□ □□□ □□ IT □□ □□□ □□ □□□ □□□□□□. □ □□□ □□□□□ □□□□ □□ □□ □□□□ □□□□ □ □□□ □ □□□□?

A. □□□ □□□□ □□ □□ □□□ □ □□ □□□□□ □□

B. □□□ □□□ □□□ □□□ □□□ □□□□□ □□

C. □□ □□□□ □□ □□□ □□□□ □□□ □□

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

Answer: B (LEAVE A REPLY)

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: 156
IS □□□□ □□ □□□ □□□□□ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□□□ □□□ □□□ □□□□□□. □□ □□ □□ □ □□ □□ □□□ □□ □□□ □□□ □ □□ □□□ □□□?
A. □□□ □□ □□ □ □□ □□ □□(NDA)□ □□□□□ □□
B. □□ □□□□ □□ □□□ □□□ □□ □□
C. □□□□□ □□ □□□□ □□□ □□□ □□ □□ □ □□ □□
D. □□□ □□ □□□□ □□ □□□□
Answer: C (LEAVE A REPLY)
The best recommendation to reduce the risk of data leakage from employee use of social networking sites for business purposes is to provide education and guidelines to employees on use of social networking sites.
Education and guidelines can help employees understand the benefits and risks of using social media for business purposes, such as enhancing brand awareness, engaging with customers, or sharing industry insights.
They can also inform employees about the dos and don'ts of social media etiquette, such as respecting privacy, protecting intellectual property, avoiding conflicts of interest, or complying with legal obligations.
Education and guidelines can also raise awareness of potential data leakage scenarios, such as phishing attacks, malicious links, fake profiles, or oversharing sensitive information, and provide tips on how to prevent or respond to them.

NEW QUESTION: 157
□□ □□□□ □ □□ □□ □□□ □□□ □□□□ □□□ □□ □□□□ □□□□□?
A. □□ □□ □□□(MTO)
B. □□ □□ □□(RPO)
C. □□□ □□ □□(SDO)
D. □□ □□□ □□ □(AIW)
Answer: A (LEAVE A REPLY)
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: 158
□□□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□ □ □□□ □ □□□□.
A. □□□ □□.
B. □□□□ □□.
C. □□ □□ □□□.
D. □□□ □□ □□□.
Answer: D (LEAVE A REPLY)
Access authorization tables are the best way to achieve effective separation of duties in an online environment, as they allow the definition and enforcement of different access rights and privileges for different users or roles, based on the principle of least privilege12. Access authorization tables can help to prevent unauthorized or inappropriate actions, such as fraud, errors, or misuse of the system, by ensuring that no user has enough privileges to perform all parts of a transaction or business process34.
References
1: Separation of Duty (SOD) - Glossary | CSRC3 2: Separation of Duties within Information Systems4 3:
Separation of Duties: Implementation & Challenges in IT2 4: Implementing Segregation of Duties: A Practical Experience Based on Best Practices - ISACA1

NEW QUESTION: 159
□□□□ □□□□ □□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□ □ □□ □□□□?
A. □□ □□ □□□ □□ □□□ □□□□□.
B. □□□ □□ □□(SLA)□ □□□□ □□ □□ □□□ □□□ □□□□□.
C. □□□ □□ □□(SLA)□□ □□□□ □□ □□□ □□□□ □□□□.
D. □□□□□ □□□ □□□□ □□ □□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 160
IS □□□□ □□□□ □□□□□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □ □ □□□□?
A. □□□□□□ □□□□ □□□□ □□□.
B. □□□ □□ □ □□□ □□□□.
C. □□□□□□ □□ □□□ □□□□□.

D. □□□ □□ □□□□□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

Reviewing the application implementation documents is the best way for an IS auditor to assess the design of an automated application control. An automated application control is a control that is embedded in the application software and is executed by the system without human intervention. An automated application control is designed to ensure the accuracy, completeness, validity, and authorization of transactions and data processed by the application. Examples of automated application controls are input validation, edit checks, calculations, reconciliations, and exception reports.

The application implementation documents are the documents that describe the design specifications, logic, and functionality of the application and its controls. The application implementation documents may include:

Business requirements document - a document that defines the business objectives, needs, and expectations of the application.

Functional specifications document - a document that describes the features, functions, and interfaces of the application and its controls.

Technical specifications document - a document that details the technical architecture, design, and configuration of the application and its controls.

Test plan and test cases - a document that outlines the testing strategy, methodology, and scenarios for verifying the functionality and performance of the application and its controls.

User manual and training material - a document that provides instructions and guidance on how to use the application and its controls.

By reviewing the application implementation documents, an IS auditor can:

Gain an understanding of the purpose, scope, and nature of the application and its controls.

Evaluate whether the application and its controls are designed to meet the business requirements and objectives.

Identify any gaps, inconsistencies, or errors in the design of the application and its controls.

Compare the design of the application and its controls with the best practices and standards in the industry.

Determine whether the application and its controls are adequately tested and documented.

Interviewing the application developer is not the best way for an IS auditor to assess the design of an automated application control. An interview is a verbal communication technique that involves asking questions and listening to responses. An interview can be useful for obtaining general information or clarifying specific issues related to the application and its controls. However, an interview alone cannot provide sufficient evidence or documentation to support the auditor's assessment of the design of an automated application control. An interview may also be subject to bias, misunderstanding, or misinterpretation by either party.

Obtaining management attestation and sign-off is not the best way for an IS auditor to assess the design of an automated application control. Management attestation and sign-off is a formal process that involves obtaining written confirmation from management that they have reviewed and approved the design of the application and its controls.
Management attestation and sign-off can indicate management's commitment and accountability for the quality and effectiveness of the application and its controls. However, management attestation and sign-off cannot substitute for an independent and objective evaluation by an IS auditor.
Management attestation and sign-off may also be influenced by pressure, conflict of interest, or fraud.
Reviewing system configuration parameters and output is not the best way for an IS auditor to assess the design of an automated application control. System configuration parameters are settings that define how the system operates or interacts with other components. System output is data or information that is produced by the system as a result of processing transactions or performing functions. Reviewing system configuration parameters and output can help an IS auditor to verify whether the system is configured correctly and whether it produces accurate and reliable output. However, reviewing system configuration parameters and output cannot provide a comprehensive view of how the application and its controls are designed to achieve their objectives. Reviewing system configuration parameters and output may also require technical expertise or access rights that may not be available to an IS auditor.

NEW QUESTION: 161
□□□□ □□□□ □□ □□□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□ □□ □□□□ □□□□. □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□(NDA)□ □□□□□ □□□□□.
B. □□ □□□ □□□(EUC)□ □□ □□ □□□ □□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The most important task before implementing any associated email controls to prevent sensitive information from being emailed outside the organization by employees is to develop an information classification scheme.
An information classification scheme is a framework that defines the categories and levels of sensitivity for different types of information, such as public, internal, confidential, or secret. An information classification scheme can help implement email controls by providing criteria and guidelines for identifying, labeling, handling, and protecting sensitive information in email attachments. The other options are not as important as developing an information classification scheme, as they do not address the root cause of the problem or provide the same benefits. Requiring all employees to sign nondisclosure agreements

(NDAs) is a legal control that can help deter or penalize employees from disclosing sensitive information, but it does not prevent them from emailing it outside the organization. Developing an acceptable use policy for end-user computing (EUC) is a governance control that can help define and communicate the rules and expectations for using IT resources, such as email, but it does not prevent employees from emailing sensitive information outside the organization. Providing notification to employees about possible email monitoring is a transparency control that can help inform and warn employees about the potential consequences of emailing sensitive information outside the organization, but it does not prevent them from doing so. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.2

NEW QUESTION: 162
□□ □ □□□□□ □□□ □□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□ □ □ □□□ □□□□□?
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: 163
IS □□□□ □□□□□ □□□□ □□□□□ □□□□ □ □□□ □□□□ □ □□ □□□ □ □□□□ □□□ □□□□, □□ □□□□ □□□□□□ □□ □□□□ □□□□□□ 6 □□□ □□ □□□□ □□□□□. □□ □ □□□□ □□ □□□ □□□□□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□?

A. □□□□□ □□□□ □□□ □□□ □□ □□□ □□□□□□ □□□□□.
B. □□□ □□□□□ □□□□□ □□□□ □□ □□ □□□ □□□□.
C. □□□ □□□□□ □□□□ □□ □□□□□□ □□□□□.
D. □□□ □□□□□ □□□□ □□□□□ □□□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
The best way to reduce the immediate risk associated with using an unsupported version of the software is to segregate the outdated software system from the main network. An unsupported software system may have unpatched vulnerabilities that could be exploited by attackers to compromise the system or access sensitive data. By isolating the system from the rest of the network, the organization can limit the exposure and impact of a potential breach. Verifying all patches have been applied to the outdated software system, closing all unused ports on the outdated software system and monitoring network traffic attempting to reach the outdated software system are also good practices, but they do not address the root cause of the risk, which is the lack of vendor support and updates.
References:
* CISA Review Manual, 27th Edition, page 2951
* CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

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

NEW QUESTION: 165
IT □□□ □□□□ □□□ □□□ □□ □□□ □□□ □□ □□□ □□□.
A. IT□ □□ □□ □□□□ □□□ □□□□.
B. IT□ □□ □□□ □□□□□□.
C. □□□ □□□ □□ □□ □□□ □□□□□.
D. IT□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Aligning IT with business strategy ensures that IT investments provide value and support business objectives.
* Option A (Incorrect):While senior management involvement is essential, it is abyproductof alignment rather than the primary goal.
* Option B (Correct):Themain purposeof alignment is tooptimize IT investmentsby ensuring that IT initiatives directly support business needs, reducing waste and improving ROI.

* Option C (Incorrect):Risk awareness is important but is not theprimaryreason for IT-business alignment.
* Option D (Incorrect):Monitoring IT effectiveness is part of governance but not the main objective of IT- business alignment.
Reference:ISACA CISA Review Manual -Domain 1: Information Systems Auditing Process- Covers IT governance, strategy alignment, and value realization.

NEW QUESTION: 166
□□ □ □□ □□□ □□□□ □□□ □□□ □□□ □□□□ □□ □ □□□□ □□ □□ □□□?
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, 27th Edition, page 401

NEW QUESTION: 167
□□ □□ □□□□ □□□ 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: 168

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

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: 169

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

A. □□ □□ □□

B. □□□ □□□ □□

C. □□□ □□

D. □□ □□ □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 170
□□□ □□□ □□□ □□□ □□ □□□□□□□ □□ □□□ □□□ □□□ □□□. □ □ □ □□ □□ IS □□□□□ □ □□□ □□□□□ □□□□□ □□□ □□□ □□□□ □?
A. □□ □□□ □□
B. □□□□□
C. □□□ □□ □□ □□ □□
D. □□ □□□ □□ □□□
Answer: (SHOW ANSWER)
Anti-malware tool audit logs would provide an IS auditor with the best evidence of continuous compliance with the global organization's policy that states that all workstations must be scanned for malware each day. Anti-malware tool audit logs are records that capture the activities and events related to the anti-malware software installed on the workstations, such as scan schedules, scan results, updates, alerts, and actions taken1. These logs can help the IS auditor to verify that the anti-malware software is functioning properly, that the scans are performed regularly and effectively, and that any malware incidents are detected and resolved in a timely manner2. Anti-malware tool audit logs can also help the IS auditor to identify any gaps or weaknesses in the anti-malware policy or implementation, and to provide recommendations for improvement3.
The other options are not the best evidence of continuous compliance with the anti-malware policy. Penetration testing results are reports that show the vulnerabilities and risks of the workstations and network from an external or internal attacker's perspective4. While penetration testing can help to assess the security posture and resilience of the organization, it does not provide information on the daily anti-malware scans or their outcomes. Management attestation is a statement or declaration from the management that they have complied with the anti-malware policy5. While management attestation can demonstrate commitment and accountability, it does not provide objective or verifiable evidence of compliance. Recent malware scan reports are documents that show the summary or details of the latest anti-malware scans performed on the workstations. While recent malware scan reports can indicate the current status and performance of the anti-malware software, they do not provide historical or comprehensive evidence of compliance.
References:
Malwarebytes Anti-Malware (MBAM) log collection and threat reports ...
Malicious Behavior Detection using Windows Audit Logs
PCI Requirement 5.2 - Ensure all Anti-Virus Mechanisms are Current ...
Management Attestation - an overview | ScienceDirect Topics
How to Read a Malware Scan Report | Techwalla

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

NEW QUESTION: 172
□□ □ □□□ □□□□ □□□ □□ □□□□ □□ □□ □□□□□?
A. □□□□ □□□ □□
B. □□ □□(QA) □□□□ □□
C. □□□□ □□□□□□ □□ □□□□ □□
D. □□ □□□□ □□□ □□
Answer: C (LEAVE A REPLY)
The best option that facilitates strategic program management is aligning projects with business portfolios (option C). This is because:
Strategic program management is the coordinated planning, management, and execution of multiple related projects that are directed toward the same strategic goals12.
Aligning projects with business portfolios means ensuring that the projects within a program are aligned with the organization's strategic objectives, vision, and mission .
Aligning projects with business portfolios helps to prioritize the most valuable and impactful projects, optimize the allocation of resources, monitor the progress and performance of the program, and deliver the expected benefits and outcomes .
Implementing stage gates (option A) is a process of reviewing and approving projects at predefined points in their lifecycle to ensure that they meet the quality, scope, time, and cost criteria. While this can help to control and improve the project management process, it does not necessarily facilitate strategic program management, as it does not address the alignment of projects with business portfolios.
Establishing a quality assurance (QA) process (option B) is a process of ensuring that the project deliverables meet the quality standards and requirements of the stakeholders. While this can help to enhance the quality and satisfaction of the project outcomes, it does not necessarily facilitate strategic program management, as it does not address the alignment of projects with business portfolios.
Tracking key project milestones (option D) is a process of monitoring and reporting the completion of significant events or deliverables in a project. While this can help to measure and communicate the progress and status of the project, it does not necessarily facilitate strategic program management, as it does not address the alignment of projects with business portfolios.

Therefore, the best option that facilitates strategic program management is aligning projects with business portfolios (option C), as this ensures that the projects within a program are consistent with the organization's strategic goals and objectives. References: 1: Program Management: The Key to Strategic Execution 2: The Ultimate Guide to Program Management [2023] * Asana : Project Portfolio Management - PMI : Aligning Projects with Strategy - Harvard Business Review : What Is Stage-Gate Process? - ProjectManager.com : Quality Assurance in Project Management - PMI : What Is a Milestone in Project Management? - TeamGantt

NEW QUESTION: 173
□□ □□□ □□□□□□ □□ □□ □ □□□ □□□□ IS □□□□ □□ □□□□ □ □ □□ □□ □ □□□□□?
A. □□ □□□ □□□□□ □□□□□ □□□□□.
B. □□ □□□□ □□ □□□ □□□□ □ □□□□.
C. □□ □□□□ □□ □□□ □□□□□□ □□□□□.
D. □□□□ □□□ □□□ □□□ □ □□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 174
□□ □□□ □□□(EUC)□□ □□ □□□ □□ □□□□□□□ □□□□ □ □□ □□ □ □□□ □□ □ □□□□□?
A. □□ □□□ □□
B. □□□□ □□ □□ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 175
□□ □□ □□ □□□ □□ □□□ □, □□□□ □□□ □□□□ □□ □□□ □□ □ □□ □□□ □□□?
A. □□ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.
B. □□ □□ □□□ □□□□ □□ □□ □□
C. □□ □□ □□□ □□ □□□□ □□ □□□ □□□□□
D. □□ □□ □□□ □□□□□□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 176
□□□□ □□ □ □□□(PKI)□ □□□□ □□□ □□□ □□□□□. □□□ □□□□ □ □ □□ □□□□□□ □□□□ □□ □□□□ □□□ □□ □ □□ □□□□?
A. □□□□ □□ □□□□□ □□□□ □□□□□□.
B. □□□□ TLS(□□ □□ □□) □□□□□ □□□□ □□□□□.

C. □□□□ □□□□ □□□□ □□□ □□ □□□□□.
D. □□□□ □□□□ □□ □□ □□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
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: 177
□□□ □□□ □□□ □□ □□□□□ □□□ □□□□ □□ IS □□□□ □□□□ □□ □□□ □□□□ □□□□□ □□ □□□□□□. □□□ □ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□□ □□□□ □□ □□ □□□ □□□□□.
B. IT □□ □□□□ □□□ □□□□ □□□□ □□ □□□ □□□□□ □□□.
C. □□ □ □□□ □□□ □□ □□□ □□□□□.
D. □□ □□ □□□ □□ □□ □□ □□□□□□□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
This is the most effective way for the organization to improve its data classification processes and procedures, because data owners are the ones who are responsible for assigning the appropriate level of classification to the data they create, collect, or manage. Data owners should be aware of the data classification policy, the criteria for each level of classification, and the implications of misclassification. IT security staff can provide tailored training for data owners based on their roles, functions, and types of data they handle.
The other options are not as effective as having IT security staff conduct targeted training for data owners:
* Use automatic document classification based on content. This is a possible option, but it may not be feasible or accurate for a small organization. Automatic document classification is a process that uses artificial intelligence or machine learning to analyze the content of a document and assign a class label based on predefined rules or models. However, this process may require a lot of resources, expertise, and maintenance, and it may not capture all the nuances and context of the data. The IS auditor should also verify the reliability and validity of the automatic document classification system.
* Publish the data classification policy on the corporate web portal. This is a good practice, but it is not enough to improve the data classification situation. Publishing the data classification policy on the corporate web portal can increase the visibility and accessibility

of the policy, but it does not ensure that data owners will read, understand, and follow it. The IS auditor should also monitor and enforce the compliance with the policy.
* Conduct awareness presentations and seminars for information classification policies. This is a useful measure, but it is not the most effective one. Conducting awareness presentations and seminars can raise the general awareness and knowledge of information classification policies among all employees, but it may not address the specific needs and challenges of data owners. The IS auditor should also provide more in-depth and practical training for data owners.

NEW QUESTION: 178
IT □□ □□□ □□□□ □□□ □□□ □□ □□□□ □□□□□□□ □□□□□ □□□ □□□□ □□ □ □□□ □□□ □□□□□ □ □□ □□ □□ □ □□□□□?
A. □□ □□□□ □□ □ □□ □□□□□□□ □□□□ □□□ □□ □ □□□□.
B. □□ □□□ □□ □□□□ □□□□□ □□□ □□ □ □ □□□□.
C. □□□□ □□□□ □□ □□□ □□□ □□□ □ □□□□.
D. □□□ □□ □□ □□□ □ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)
Consolidating mission-critical applications onto a single large server introduces a single point of failure. If the server experiences an outage, all hosted applications could be impacted simultaneously, leading to significant operational disruptions. While continuous monitoring costs, potential network bandwidth issues, and challenges in capacity forecasting are valid concerns, the risk of a single outage affecting multiple critical applications presents the most substantial threat to business continuity.
References:
* ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

NEW QUESTION: 179
□□ □ □□ □□□ □□□ □ □□□ □□□□ □□□□□□ □□□□ □ □□ □□□ □ □□ □□□ □□□□□?
A. □□ □□□
B. □□ □□□
C. □□ □□□
D. □□ □□□
Answer: (SHOW ANSWER)
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: 180
□□□□ □□□ □□□ □□ □□ □□ □□□ □□□ □□□ □□ □ □□ □ □□ □□□ □□ □□□□□?
A. □□□ □□□ □□ □ □□□ □□□□ □□□ □□□□□□.
B. □□ □□□ □□ □□□ □□ □□□ □□□ □□ □□□ □□□□.
C. □□ □□□□ □□ □□ □□□ □□□□□ □□□□ □□□□□.
D. □□□ □□ □□ □□□ □□□ IT □□□□ □□□□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The most useful thing to do when planning to audit an organization's compliance with cybersecurity regulations in foreign countries is to map the different regulatory requirements to the organization's IT governance framework. This is because an IT governance framework is a roadmap that defines the methods used by an organization to implement, manage and report on IT governance within said organization1. IT governance helps align business and IT strategies using a solid and formal framework2. By mapping the different regulatory requirements to the IT governance framework, the auditor can: Identify the commonalities and differences among the various cybersecurity regulations that apply to the organization's operations in different countries.

Assess the level of compliance and maturity of the organization's IT governance practices against each regulatory requirement.
Evaluate the risks and gaps associated with non-compliance or partial compliance with any of the regulatory requirements.
Recommend appropriate actions or improvements to enhance the organization's IT governance and cybersecurity posture.
Option D is correct because mapping the different regulatory requirements to the organization's IT governance framework is a systematic and effective way to plan and conduct an audit of compliance with cybersecurity regulations in foreign countries.

NEW QUESTION: 181
□□□□ □□□□□□□ □□ □□□ □□□ □□□□□, □□□ □□□□ □□□ □□□ □ □□□□□ □□□□□□. □□ □ BEST □□□ □□□□□ □□□□□□ □□□ □□ □□ □□ □□□□□?
A. □□ □□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□.
B. □□ □□□ □□ □□□□ □□□ □□□ □□□ □□□□□.
C. □□ □□□□ □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
D. □□□□ □□□□ □□ □□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
Recounting the transaction records to ensure no records are missing provides assurance that the best transactions were recovered successfully from a snapshot copy. This is because recounting the transaction records can verify that the number of records in the restored database matches the number of records in the snapshot copy, which represents the state of the database before the deletion occurred. Recounting the transaction records can also detect any data corruption or inconsistency that may have occurred during the restore process1.
Reviewing transaction recovery logs to ensure no errors were recorded is not the best answer, because transaction recovery logs may not capture all the details or issues that may affect the data quality or integrity. Transaction recovery logs are mainly used to monitor and troubleshoot the restore process, but they may not reflect the actual content or accuracy of the restored data2.
Rerunning the process on a backup machine to verify the results are the same is not the best answer, because rerunning the process may introduce additional errors or inconsistencies that may affect the data quality or integrity. Rerunning the process may also consume more time and resources than necessary, and it may not guarantee that the results are identical to the original data3.
Comparing transaction values against external statements to verify accuracy is not the best answer, because external statements may not be available or reliable for all transactions. External statements are documents or reports that provide information about transactions from a third-party source, such as a bank, a vendor, or a customer. However,

external statements may not cover all transactions, or they may have different formats, standards, or timeliness than the internal data

NEW QUESTION: 182
□□ □□ □□□ □□ □□ □□ □□(QA)□ □□□□ □□ □□□ □□□ □□□□ □□ □□□□.
A. □□ □□□□ □□ □□□□□ □□□□□.
B. □□ □□ □□□ □□ □□ □ □□□□ □□□□□.
C. □□ □□□ □□□□ □□□□ □□ □□□ □□□□□.
D. □□□ □□□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
The primary reason to perform internal QA for an internal audit function is to ensure that the internal audit activity adheres to the Definition of Internal Auditing and the International Standards for the Professional Practice of Internal Auditing (Standards) issued by the Institute of Internal Auditors (IIA), as well as the internal audit methodology and policies of the organization. A QA program enables an evaluation of the internal audit activity's performance, efficiency, effectiveness, and value, and identifies opportunities for improvement. A QA program also helps to enhance the credibility and reputation of the internal audit function among the stakeholders.
References
Quality Assurance - The Institute of Internal Auditors or The IIA
Benefits of a quality assurance review for internal audit
Optimize your internal audit function with a quality assurance review ...

NEW QUESTION: 183
□□ □□ □□□ □□ □□ □□ □□□ □□□□ □ □□□ □□ □□□ □□□ □□ □ □ □ □□□?
A. □□□ □□□ □□□ □□□ □□□□ □□ □□ □□□□ □□ □□□ □□ □□□ □ □□□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□
B. □□ □□□□ □□□ □□□ □□□ □□□□□□ □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 184

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

A. IT □□□□ □□ □□□ □□□□□ □□□□ □□ □□ □□□□□ □□□ □□□□□.

B. □□□ □□□□□ □□□ □□ □□□□ □□□□□□□.

C. □□□ □□□ □□ □□□ □□□□ □□□ □□□□□.

D. IS □□ □□□□ □□ □□□ □□□□□ □□ □□ IS □□□□ □□□□□ □□□□ □□□.

Answer: B (LEAVE A REPLY)

Outsourcing the audit to independent and qualified resources is the best course of action for the IS audit manager who was temporarily tasked with supervising a project manager assigned to the organization's payroll application upgrade. This is because the IS audit manager has a potential conflict of interest and a threat to objectivity and independence, which are essential principles and standards for IS auditors.

According to the ISACA Code of Professional Ethics, IS auditors should maintain objectivity and independence in their professional judgment and avoid any situations that may impair or be presumed to impair their objectivity or independence1. Objectivity is the mental attitude of an IS auditor that allows them to perform their work honestly, impartially, and with integrity, while independence is the freedom from conditions that threaten the ability of an IS auditor to carry out their work in an unbiased manner2.

The IS audit manager who was involved in supervising the payroll application upgrade project may have a self-review threat, which is the risk that an IS auditor will not appropriately evaluate the results of a previous judgment made or service performed by them or their subordinates3. The IS audit manager may also have a familiarity threat, which is the risk that an IS auditor will be influenced by a close relationship with someone involved in the project or by their own personal interests4. These threats may compromise the IS audit manager's objectivity and independence and affect the quality and credibility of the audit.

Therefore, the IS audit manager should disclose their involvement in the project to their senior management and the audit committee and decline to perform or manage the audit. The IS audit manager should also recommend outsourcing the audit to independent and qualified resources who have no connection or interest in the project and who have the necessary skills and experience to conduct a reliable and effective audit.

The other options are not the best course of action for the IS audit manager.

Transferring the assignment to a different audit manager despite lack of IT project management experience is not the best course of action because it may result in a low-quality audit that does not meet the expectations and standards of the stakeholders. IT project management experience is essential for auditing an IT project, as it requires knowledge of project management methodologies, tools, techniques, risks, and best

practices. An audit manager who lacks IT project management experience may not be able to plan, execute, report, and follow up on the audit effectively and efficiently.
Managing the audit since there is no one else with the appropriate experience is not the best course of action because it violates the ethical principles and standards of objectivity and independence for IS auditors.
Managing the audit would create a conflict of interest and a threat to objectivity and independence for the IS audit manager, as they would be reviewing their own work or that of their subordinate. Managing the audit would also undermine the credibility and reliability of the audit results and recommendations, as they may be biased or influenced by personal or professional relationships or interests.
Having a senior IS auditor manage the project with the IS audit manager performing final review is not the best course of action because it still involves the IS audit manager in the audit process, which poses a conflict of interest and a threat to objectivity and independence. Performing final review would require the IS audit manager to evaluate and approve the work done by the senior IS auditor, which may be affected by their previous involvement in or knowledge of the project. Performing final review would also expose theIS audit manager to undue pressure or influence from management or other stakeholders who may have expectations or preferences regarding the audit outcome.

NEW QUESTION: 185
IS □□□□ □□□ □□□ □□ □□□ □□□□ □□□□. □□ □□ □ □□ □□ □□□ □□ □□□ □□□ □ □□□□?
A. □□ □□□ □□ □□□ □□
B. □□□□ □□□ □□□□□ □□ □□
C. □□□ □□ □□□ □□ □□□□ □□
D. □□ □□ □□□ □□ 2□□
Answer: (SHOW ANSWER)
An IS auditor is conducting a review of a data center. An observation that could indicate an access control issue is muddy footprints directly inside the emergency exit. Access control is a process that ensures that only authorized entities or individuals can access or use an information system or resource, and prevents unauthorized access or use. Access control can be implemented using various methods or mechanisms, such as physical, logical, administrative, etc. Muddy footprints directly inside the emergency exit could indicate an access control issue, as they could suggest that someone has entered the data center through the emergency exit without proper authorization or authentication, and potentially compromised the security or integrity of the data center. Security cameras deployed outside main entrance is not an observation that could indicate an access control issue, but rather a control that could enhance access control, as security cameras are devices that capture and record video footage of the surroundings, and can help monitor and deter unauthorized access or activity. Antistatic mats deployed at the computer room entrance is not an observation that could indicate an access control issue, but rather a control that

could prevent static electricity damage, as antistatic mats are devices that dissipate or reduce static charges from people or objects, and can help protect electronic equipment from electrostatic discharge (ESD). Fencing around facility is two meters high is not an observation that could indicate an access control issue, but rather a control that could improve physical security, as fencing is a barrier that encloses or surrounds an area, and can help prevent unauthorized entry or intrusion.

NEW QUESTION: 186
□□ □□ □□□□ □□□□ □□ □□□□ □□□□□□ □□□□ □□□□ □□□ □ □ □ □□□ □□□□ □□□ □□□□□ □□ □□□□□□. IS □□□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□ □□ □□□ □□ □□
B. □□□□ □□ □□□ □□□□ □□ □□□□
C. □□□□□ □□ □□ □□□ □□□□ □□□□□ □□
D. □□□□ □□ □□□ □□□□ □ □□ □□□ □
Answer: B (LEAVE A REPLY)
The IS auditor should review the processes for making changes to cloud environment specifications, as these are the inputs for the predefined automated procedures that deploy and configure the application infrastructure. The IS auditor should verify that the changes are authorized, documented, tested, and approved before they are applied to the cloud environment. The IS auditor should also check that the changes are aligned with the business requirements and do not introduce any security or performance issues.
References
ISACA CISA Review Manual, 27th Edition, page 254
Configuration Management in Cloud Computing - ScienceDirect
Cloud Configuration Management - BMC Software

NEW QUESTION: 187
□□□□ □□□□□□ □□□□□ □□□□ □□□ □□ □□□ □□□□ □□□.
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: 188
□□□ □□ □□(DLP) □□□ □□□ □□ □ □□□ □□□ □ □□ □□ □□□□ □ □ □□ □□□□□?
A. □□□ □□□ □□ □□ □□
B. □□□ □□□ □□
C. □□□ □□□ □□ □□ □□
D. □□□ □□□□ □□ □□
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
ADLP strategyaims toprevent data breachesby ensuringusers handle data securely.
* Option A (Incorrect):Avoiding financial and reputational risk is anoutcome, but not theprimary goal of training.
* Option B (Incorrect):Data availabilityis important but is notdirectly relatedto DLP user training.
* Option C (Correct):User training should focus on secure data handling, as human error is a leading cause of data loss incidents.
* Option D (Incorrect):Data governanceensurescompliance, but secure handling practices are themain goal of DLP training.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-CoversDLP strategies, security awareness, and training.

NEW QUESTION: 189
IS □□□□ □□□□ □ □, □□ □□ □□□ □□□□□□ □□□□□ □□□□ □□ □ □□ □ □□ □□ □ □□□ □□□□□?
A. □□ □□□□ □□□□ □□ □□□ □□ □ □□
B. □□ □□□ □□□□ □□ □□□□□ □□□ □ □□
C. □□□□□ □□ □□□ □□□ □ □□
D. □□□ □□□□□ □□□ □□□ □ □□
Answer: (SHOW ANSWER)
The greatest risk associated with an incomplete inventory of deployed software in an organization is the inability to deploy updated security patches. Security patches are updates that fix vulnerabilities or bugs in software that could be exploited by attackers. Without an accurate inventory of software versions and config urations, it is difficult to identify and apply the relevant patches in a timely manner, which exposes the organization to increased security risks. Inability to close unused ports on critical servers, inability to identify unused licenses within the organization, and inability to determine the cost of

deployed software are not as critical as security risks. References: ISACA CISA Review Manual 27th Edition, page 308

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

NEW QUESTION: 191
□□□□ □□□□ □□ □□ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□□ □□(SIEM) □□ □□□□
B. □□□□ □□ □□□ □□ □□
C. □□□□ □□ □□□□□ □□□
D. □□ □□ □□□(IDS)□ □□
Answer: C (LEAVE A REPLY)
An external assessment of network vulnerability is a process of identifying and evaluating the weaknesses and risks that affect the security and availability of a network froman outsider's perspective. The most important factor to verify during this process is the completeness of network asset inventory, which is a list of all the devices, systems, and software that are connected to or part of the network. A complete and accurate network asset inventory can help identify the scope and boundaries of the network, the potential attack vectors and entry points, the critical assets and dependencies, and the existing security controls and gaps. Without a complete network asset inventory, an external assessment of network vulnerability may miss some important assets or vulnerabilities, leading to inaccurate or incomplete results and recommendations.
References:
* 1 explains what is an external vulnerability scan and why it is important to have a complete network asset inventory.
* 2 provides a guide on how to conduct a full network vulnerability assessment and emphasizes the importance of knowing the network assets.
* 3 compares internal and external vulnerability scanning and highlights the need for a comprehensive network asset inventory for both types.

NEW QUESTION: 192
IS □□□□ □□□□ □□ □□□ □ □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□. □□ □ □□□□□ □□ □ □□□□ □□□□□?
A. □□□□ □□□□□ □□□ □□□□ □□□ □□□□□□.
B. □□□ □□□□ □ □□□ □□□ □□□ □□□ □ □□ □□□□ □□□□□.

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

NEW QUESTION: 193
□□ □ □□□□□ IT□ □□□□ □ □□ □ □□□ □□□□ □□ □□□□□?
A. □□□ □□□ □□□□□□□(CIO)□ □□□□ □□
B. □□□ □□ □□□□□ □□□□□ IT □□□ □□□□□.
C. □□□□ □□ □□□ □□ □□ □□ □□
D. □□□□□□□(CIO)□ □□□ □□ IT □□□□□
Answer: A (LEAVE A REPLY)
The greatest challenge to the alignment of business and IT is the lack of chief information officer (CIO) involvement in board meetings. The CIO is the senior executive responsible for overseeing the IT strategy, governance, and operations of the organization, and ensuring that they support the business objectives and needs. The CIO should be involved in board meetings to communicate the value and contribution of IT to the organization, to align the IT vision and direction with the business strategy and priorities, and to advocate for the IT resources and investments required to achieve the desired outcomes. The lack of CIO involvement in board meetings can result in a disconnect between business and IT, a loss of trust and confidence in IT, and missed opportunities for innovation and value creation. The other options are not as challenging as the lack of CIO involvement in board meetings, because they either do not affect the strategic alignment of business and IT, or theycanbe addressed by other means such as collaboration, negotiation, or escalation. References: CISA Review Manual (Digital Version)1, Chapter 1, Section 1.2.1

NEW QUESTION: 194
□□ □ □□ □□□□□□□ □□ □□□□ □□ □□ □□□ □ □□ □□ □□□ □□□ □ □□ □□□□□?
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: 195
□□□ □□□□ 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: 196
□□ □□ □□□□ □□□ □, □□□ □□□ □□ □□□□ □□ □□ □□□ □□□ □□ □□□?
A. □□ □□□□ □□□ □□□ □□□□ □□□□□ □□
B. □□□ □□□ □□ □□□□ □□ □□ □□
C. □□□ □□□ □□ IT □□ □□□ □□
D. IT □□□ □□□ □□□□ □□□ □□□□ □□ □□
Answer: B (LEAVE A REPLY)
Obtaining management's consent to the testing scope in writing is the most important step prior to finalizing the scope of testing, as it ensures that the penetration testers have the

authorization and approval to perform the testing activities. It also protects them from any legal liabilities or accusations of unauthorized access or damage. The other options are not as important as obtaining management's consent, and they may vary depending on the specific situation and agreement. For example, some systems may not be excluded from the testing scope, and some tests may not be restricted to the test environment.
References: CISA Review Manual (Digital Version) 1, page 381-382.

NEW QUESTION: 197
□□□□ □□□ □□□ □ □□ □□□ □□ □□□□□ □□ □□, □□□ □□□ □□□ □ □□□□ □□ □□ □□□ □□ □ □□ □□□?
A. □□ □□□ □□ □□□ □□
B. □□□ □□□ □□ □□ □□
C. □□ □□□ □□ □□□ □□ □□□ □□
D. □□ □□□ □□□ □□ □□
Answer: (SHOW ANSWER)
Source code synchronization is the process of ensuring that the source code and the object code (the compiled version of the source code) are consistent and up-to-date1. When program changes are implemented, the source code should be recompiled to generate a new object code that reflects the changes. However, if the source code is not recompiled, there is a risk that the object code may be outdated or incorrect. A compensating control is a measure that reduces the risk of an existing control weakness or deficiency2. A compensating control for source code synchronization is to compare the date stamping of the source and object code. Date stamping is a method of recording the date and time when a file is created or modified3. By comparing the date stamping of the source and object code, one can verify if they are synchronized or not. If the date stamping of the source code is newer than the object code, it means that the source code has been changed but not recompiled. If the date stamping of the object code is newer than the source code, it means that the object code has been compiled from a different source code. If the date stamping of both files are identical, it means that they are synchronized.

NEW QUESTION: 198
□□ □□□ □□□□ □ □□□ □□ □□□ □□□ □□□ □ □□ □□□ □□□□□ □ □□□□?

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

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

NEW QUESTION: 200
IS □□□□ □□ □□□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□□ □□ □□ □□□.
□□□ □□ □□□ □□ □□□ □□□ □□□□ □□ □□ □□ □□ □□□ □□□□□?
A. □□ □□
B. □□□□□
C. □□ □□ □□
D. □□ □□□
Answer: (SHOW ANSWER)
Clustering is a technique that allows multiple servers to work together as a single system, providing high availability, load balancing, and fault tolerance. Clustering can limit the potential impact of server failures in a distributed environment, as it can automatically switch the workload to another server in the cluster if one server fails, without interrupting the service. Redundant pathways, failoverpower, and parallel testing are also useful for improving the reliability and availability of servers, but they do not directly address the issue of server failures.

NEW QUESTION: 201
□□ □□□ □□□ □□□ □□ □□□ □□□ □ 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: 202
□□□ □□ □□□□ □□□□ □□ □ □□□ □□□ □□□ □□ □□□□ □□□ □□ □ □□□□□.
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: 203
□□□□□□ 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: 204
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: 205
□□□□□□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □□ □ □□ □□□□ □ □ □□□ □□□ □□□□□?
A. □□□ □□ □□□(UAT)
B. □□□□ □□□
C. □□□□□ □□□
D. □□ □□□
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
White box testingis the most effective foridentifying hidden errorsand optimizingsource code quality.
* Option A (Incorrect):UAT focuses on functionalityfrom anend-user perspective, not source code errors.
* Option B (Incorrect):Black box testingexamines software behaviorwithout reviewing code, making it less effective for code-level optimization.
* Option C (Correct):White box testing(also known asclear box or structural testing)analyzes source codefor vulnerabilities, logic errors, and optimization opportunities.
* Option D (Incorrect):Penetration testingidentifiessecurity weaknesses, but it does notfocus on code efficiency.
Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Coverssoftware testing methodologies and secure coding practices.

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

NEW QUESTION: 207
IS □□□□ □□ □□□□□□ □□□□ □□□□ □□ RFP□ □□□ □□□□ □□□□.
□□□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□□□ □□□ □□ □□□ □□□□ □□□.
B. □□ □□ □□□ □□□ □□□□ □□□.
C. □□□ □□□□□ □□ □□□ □□ □□□ □□□ □□□.
D. □□□□ □□□ □□□□□ □□□□□ □□□□ □□□.
Answer: B (LEAVE A REPLY)
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: 208
IS □□□□ □□ □□□□□ □□□□□□ ERP(Enterprise Resource Planning) □□□□ □□□ □□□□ □□□□.
□□□□ □□ □□□ □□□□ □□□?
□ □□□□□ □□□ □□□□□?
A. □□□□□□□
B. □□□□□□ □□□(DBA)
C. □□ □□□
D. □□□ □□□□
Answer: C (LEAVE A REPLY)
The best option for the question is C, information owner. This is because:

The information owner is the person or entity that has the authority and responsibility for the business processes and functions that collect, use, store, and dispose of data1.
The information owner is 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.
The information owner is 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.
The information owner 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.
Therefore, the information owner should be responsible for the data classification in an ERP migration project from local systems to the cloud (option C), as they have the authority and accountability for the data and its protection.
The other options are not correct because:
The information security officer (option A) is responsible for overseeing and coordinating the security policies and practices of the organization that involve data6. The information security officer should advise and assist the information owner on the best practices and standards for data security, but not determine the data classification.
The database administrator (DBA) (option B) is responsible for installing, configuring, monitoring, maintaining, and improving the performance of databases and data stores that contain data5. The DBA should support the information owner in implementing and enforcing the data classification policies and procedures, but not determine them.
The data architect (option D) is responsible for designing, modeling, and documenting the logical and physical structures of databases and data stores that contain data7. The data architect should collaborate with the information owner in creating and maintaining the data classification schema and metadata, but not determine them.

NEW QUESTION: 209
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: 210

□□ □□□□ □□ □□□ □□□□ □□ □□(RAID)□ □□□□ □□□□ □□□□ IS □ □□□ □□□□□ □□□ □□□□ □□ □□□ □□□ □□□□□?

A. □□□ □□ □□□□□ □□□ □ □□□□.

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

NEW QUESTION: 211
□□ IT □□□ □□□□□ □□□□ □□□ □□(HR) □□□□ □□□□□ □□□ □□□ □□□ □□ IS □□□□ □□ □□ □□□□ □□□□□?
A. □□□□□ □□□□□.
B. □3□ □□ □□□□ □□□□□.
C. □□ □□ □□□ □□□□□.
D. □□□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
The best recommendation for an IS auditor when finding that a third-party IT service provider hosts the organization's HR system in a foreign country is to conduct a privacy impact analysis. A privacy impact analysis is a systematic process that identifies and evaluates the potential risks and impacts of collecting, using, disclosing, and storing personal information. A privacy impact analysis will help the IS auditor to assess the legal, regulatory, contractual, and ethical obligations of the organization and the service provider regarding the protection of personal information. A privacy impact analysis will also help to identify and mitigate any privacy risks and gaps in the service level agreement.
References:
* CISA Certification | Certified Information Systems Auditor | ISACA
* CISA Questions, Answers & Explanations Database

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

B. □□ □□□ □□□ □□□
C. □□□□□ □□□□□ □□
D. □□□□ □□□ □□□ □□□ □□□
Answer: B (LEAVE A REPLY)
To ensure that management concerns are addressed, internal audit should recommend that the data quality team review the data reported to the regulatory body first. This is because this data set is the most relevant and critical to the issue that triggered the enhancement of the data quality program. The data reported to the regulatory body should be accurate, complete, consistent, and timely, as any discrepancies could result in fines, penalties, or reputational damage for the organization.Data with customer personal information is important for data quality, but it is not directly related to the regulatory reporting issue. Data supporting financial statements is important for data quality, but it may not be the same as the data reported to the regulatory body. Data impacting business objectives is important for data quality, but it may not be as urgent or sensitive as the data reported to the regulatory body. References:
* CISA Review Manual, 27th Edition, pages 404-4051
* CISA Review Questions, Answers & Explanations Database, Question ID: 262

NEW QUESTION: 213
□□ □□□ □3□□ □□□□ □□ □□□□□ □□ □□ □□□ □□□□□□.
□□□□□ □□□ □□ □□ □□□ □□ □□□□□?
A. □□ □ □□□□□ □□□□ □□ □□ □□
B. □□□ □□ □□□ □□□ □□□ □□□□□ □□
C. □□□ □□ □□□□ □□□□ □□□
D. □□□□□ □□ □□ □□□□□ □□□□□□ □□
Answer: C (LEAVE A REPLY)
Before sending backup drives to an offsite storage facility, the most important thing to do is to encrypt the drive with strong protection standards. This is because encryption ensures effective security where information cannot be intercepted and used to harm the organization or its customers. Encryption also protects the data from unauthorized access, modification, or deletion in case the drive is lost, stolen, or damaged during transit or storage. Encryption of backup drives is especially important for public safety organizations that handle sensitive or personally identifiable information, such as medical records, criminal records, or emergency communications12.

NEW QUESTION: 214
□□□ □□ □□□□□ □□□□ □□ □□□□ □□ □□□ □□ □□□□. □□ □□ □ □□ □□ □□ □ □□□ □□□ □□ □□ □ □□□ □□□□□?
A. □□ □□ □□□□ □□ □□ □□□ □□□□ □□□□□.
B. □□□ □□□ □□ □□□ □□□□ □□□□ □□□□□□.
C. □□□ □□□ □□□□□ □□ IS □□□ □□□□□.

D. □□ □□ □□□ □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

The strategy that would provide the greatest assurance of system quality at implementation is delivering only the core functionality on the initial target date. This strategy can help avoid compromising the quality of the system by focusing on the essential features that meet the user needs and expectations. Delivering only the core functionality can also help reduce the scope creep, complexity, and testing efforts of the system development project.

Implementing overtime pay and bonuses for all development staff, utilizing new system development tools to improve productivity, and recruiting IS staff to expedite system development are not strategies that would provide the greatest assurance of system quality at implementation. These strategies may help speed up the system development process, but they may also introduce new risks or challenges such as burnout, learning curve, integration issues, or communication gaps. These risks or challenges may adversely affect the quality of the system.

NEW QUESTION: 215

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

A. □□□□ □□

B. □□ □□□□□□ □□□ □□ □□□□□

C. □□ □□□ □□ □□

D. □□ □□(QA) □□□ □□ □□

Answer: B (LEAVE A REPLY)

Parallel simulation involves running the same data through two systems and comparing the results1. In this case, the bank's data would be processed using both the modified interest calculation program and an audit software. The results from both systems would then be compared to check for discrepancies1. This technique provides strong evidence of the correctness of interest calculations as it directly tests the program's output against a known and trusted output1. While source code review23, manual verification of a sample of results4567, and review of QA test results8910 can also provide valuable insights, they do not offer the same level of direct, comparative evidence as parallel simulation1.

References:

Parallel simulation in IT testing - Universal CPA Review

5 code review best practices - Work Life by Atlassian

How to Make Good Code Reviews Better - Stack Overflow

Guidelines for the validation and verification of quantitative and qualitative test methods - Mathematics LibreTexts Method Validation and Verification - University of Utah Sample Procedure for Method Validation - NIST Method validation and verification - CFS Good Practices for Quality Assurance Reviewers: Assessing Evidence of Supervisory Review - IGNET How do quality assurance engineers test calculations? - Software Quality

Assurance & Testing Stack Exchange Quality Assurance/Quality Control (QA/QC) Plan and Procedures - UNFCCC

NEW QUESTION: 216
□□ □□ □ □□ □□□ □□□□ □□ □□□ □□□□ □□□ □□□ □□□□ □ □□ □□□□□?
A. □□□□ □□ □□□ □□ □□□
B. □□□ □□□
C. □□ □□
D. □□ □□□ □□
Answer: (SHOW ANSWER)
Ahardware-based media write blocker(Option A) ensures that forensic investigators can acquire digital evidencewithout altering the original data, maintaining its integrity for legal proceedings.
ISACA CISA Reference:Digital forensics best practices emphasize write-blocking devices to prevent contamination of evidence.
Risk Implication:Without a write blocker, evidence may be tampered with, compromising its admissibility in court.

NEW QUESTION: 217
□□□ □□□ □□□□ □□□ □□ □□(DLP) □□□□ □□□ □ □□ □□ □□□ □ □ □□ □□□□□?
A. □□□ □□□□ □ □□ □□□ □□□□□.
B. □□ □□□□ □□□ □□□ □□□□ □□
C. □□□ □□□ □□□ □□ □□ □□□ □□□□□.
D. DLP □□ □ □□□ □□
Answer: A (LEAVE A REPLY)
The first step when developing a DLP solution for a large organization is to conduct a data inventory and classification exercise. This step involves identifying and locating all the data assets that the organization owns, generates, or handles, and assigning them to different categories based on their sensitivity, value, and regulatory requirements1. Data inventory and classification is essential for DLP because it helps to determine the scope and objectives of the DLP solution, as well as the appropriate level of protection and monitoring for each data category2. Data inventory and classification also enables the organization to prioritize its DLP efforts based on the risk and impact of data loss or leakage3.
Option B is not correct because identifying approved data workflows across the enterprise is a subsequent step after conducting data inventory and classification. Data workflows are the processes and channels through which data are created, stored, accessed, shared, or transmitted within or outside the organization4. Identifying approved data workflows helps to define the normal and legitimate use of data, as well as to detect and prevent

unauthorized or anomalous data activities5. However, before identifying approved data workflows, the organization needs to know what data it has and how it should be classified.
Option C is not correct because conducting a threat analysis against sensitive data usage is another subsequent step after conducting data inventory and classification. Threat analysis is the process of identifying and assessing the potential sources, methods, and impacts of data loss or leakage incidents. Threat analysis helps to design and implement effective DLP controls and countermeasures based on the risk profile of each data category. However, before conducting threat analysis, the organization needs to know what data it has and how it should be classified.
Option D is not correct because creating the DLP policies and templates is the final step after conducting data inventory and classification, identifying approved data workflows, and conducting threat analysis. DLP policies and templates are the rules and configurations that specify how the DLP solution should monitor, detect, report, and respond to data loss or leakage events. DLP policies and templates should be aligned with the organization's business needs, regulatory obligations, and risk appetite. However, before creating the DLP policies and templates, the organization needs to know what data it has, how it should be classified, how it should be used, and what threats it faces.
References:
Data Inventory & Classification: The First Step in Data Protection1
Data Classification: What It Is And Why You Need It2
How to Prioritize Your Data Loss Prevention Strategy in 20203
What Is Data Workflow? Definition & Examples4
How to Identify Data Workflows for Your Business5
Threat Analysis: A Comprehensive Guide for Beginners
How to Conduct a Threat Assessment for Your Business
What Is Data Loss Prevention (DLP)? Definition & Examples
How to Create Effective Data Loss Prevention Policies

NEW QUESTION: 218
□□□□□ □□ □□□ □□□□ □□ □□□□ □□□□□□ □□□ □□ □□□ □□□ □ □□ □□ □□□□?
A. □□ □□□□ □□□□ □□□□ □□ □□ □□
B. □□□□□□ □□ □□ □□□□ □□□ □□□□□□□.
C. □□□ □□□□□ □□□ □ □□□ □□ □□□(UAT) □□
D. □□□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□□□ □□ □□
Answer: B (LEAVE A REPLY)
The best phase of the software development life cycle to initiate the discussion of application controls is the application design phase when process functionalities are finalized. Application controls are the policies, procedures, and techniques that ensure the completeness, accuracy, validity, and authorization of data input, processing, output, and storage in an application. Application controls help prevent, detect, or correct errors and

fraud in software applications. Examples of application controls include input validation, edit checks, reconciliation, encryption, access control, audit trails, etc.
The application design phase is when the software requirements are translated into a logical and physical design that specifies how the application will look and work. This phase is the best time to discuss application controls because it allows the developers to incorporate them into the design specifications and ensure that they are aligned with the business objectives and user needs. By discussing application controls early in the design phase, the developers can also avoid costly rework or changes later in the development process.
The other phases are not as optimal as the application design phase to initiate the discussion of application controls. A. Business case development phase when stakeholders are identified. The business case development phase is when the feasibility, scope, objectives, benefits, risks, and costs of a software project are defined and evaluated. This phase is important for obtaining stakeholder approval and support for the project, but it is too early to discuss application controls in detail because the software requirements and functionalities are not yet clear or finalized. B. User acceptance testing (UAT) phase when test scenarios are designed. The user acceptance testing phase is when the software is tested by the end-users or stakeholders to verify that it meets their expectations and requirements. This phase is too late to discuss application controls because it is near the end of the development process and any changes or additions to the application controls would require retesting and revalidation of the software. C. Application coding phase when algorithms are developed to solve business problems. The application coding phase is when the software design is translated into executable code using programming languages and tools. This phase is not ideal to discuss application controls because it is after the design phase and any changes or additions to the application controls would require redesigning and recoding of the software.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* What Is Application Control? | McAfee3
* What Is Application Lifecycle Management? | Red Hat4

NEW QUESTION: 219
□□ □□□□□□ □□ □□□□□ □□ □□□ □□□□ □□ IS □□□□ □□□ □□ □□□□□ □□□□ □□□ □□□ □□□□ □□□□ □□□□.
A. □□ □□□□ □□□ □□□.
B. □□ □□□.
C. □□-□□ □□.
D. □□□□ □□.
Answer: A (LEAVE A REPLY)

Reviewing and evaluating application test cases is the most effective use of an IS auditor's time during the evaluation of controls over a major application development project. Application test cases are designed to verify that the application meets the functional and non-functional requirements and specifications. They also help to identify and correct any errors, defects, or vulnerabilities in the application before it is deployed. By reviewing and evaluating the test cases, the IS auditor can assess the quality, reliability, security, and performance of the application and provide recommendations for improvement.

NEW QUESTION: 220
□□ □ □□ □□□ □□□□□?
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: 221
□□□ □□□□□ □□ □□□□ □□□□ □□ □□ □□□ □□□□□□□. □□ □ □ □ □□□ □□□ □□□□□?
A. □□□□ □□ □□ □□□(IDS)□ □□ □□Ł□□ □ □□□ □□□□□ □ □□
B. □□ □□□□ □□□ □□□ □□□ □□□□ □□□
C. □□□ □□ □□ □□□ □ □□□ □□□□ □□
D. □□□ □□□ □□□□□ □□□ □□□ □□□□□□ □□
Answer: A (LEAVE A REPLY)
The most significant risk in virtualizing the server environment without making any other changes to the network or security infrastructure is the inability of the network intrusion detection system (IDS) to monitor virtual server-to-server communications. This can create blind spots for the IDS and allow malicious traffic to bypass detection. A vulnerability in the virtualization platform affecting multiple hosts is a potential risk, but not necessarily more significant than the loss of visibility. Data center environmental controls not aligning with new configuration or system documentation not being updated to reflect changes in the

environment are operational issues, not security issues. References: ISACA, CISA Review Manual, 27th Edition, 2018, page
373

NEW QUESTION: 222
□□□□ □□ □□□□□ □□□□ □□ □□□□□ □□□ □□□□□□□ □□□□□ □□□. IS □□□□ □□□□ □□□□ DNS(□□□ □□ □□□) □□□□□ □□□□ □ □ □□ □ □□ □□ □□□□ □□□?
A. □□□□ DNS □□□□ □□□□ □□ □□□□ □□ □□□ □□□ □□□□□□.
B. □□□ □□ □□□ □□ □□□ □□□ □□□ □□□□□ ONS □□□ □□□□□.
C. DNS □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□ □□□□ □□ □ □□□□ □□□□□.
D. DNS □□ □□□ □□□ □□□□ □□□ □□ □□ □□□ □□□□□ □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 223
IT □□ □□ □□ □□(RTO)□ □□□ □□□□ □□ □□□.
A. □□ □□□ □□ □□□ □□□.
B. □□□ □□
C. □□ □□ □□ □□ □□(MTD).
D. □□□□ □□□□ □□ □□□.
Answer: D (LEAVE A REPLY)
IT disaster recovery time objectives (RTOs) are the maximum acceptable time that an IT system can be unavailable after a disaster before it causes unacceptable consequences for the business. IT RTOs should be based on the business-defined criticality of the systems, which reflects how important they are for supporting the business processes and functions. The maximum tolerable loss of data, the nature of the outage, and the maximum tolerable downtime (MTD) are also factors that affect the IT RTOs, but they are not the primary basis for determining them.

NEW QUESTION: 224
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: 225
□□ □□□ □□□(EUC)□□ □□□ □□□ □□□ □□ □□□□ □ □□ □□□ □□□ □ □□ □□ □□□ □□ □ □□□□□?

A. □□□□ □□□□ □□ □□□ □□□□□ □□□.
B. □□ □□□□□□□ EUC □□□□ □□□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. □□ □□□ □□ EUC □□ □□
Answer: B (LEAVE A REPLY)
The best way to mitigate the risk associated with unintentional modifications of complex calculations in end- user computing (EUC) is to execute copies of EUC programs out of a secure library. This will ensure that the original EUC programs are protected from unauthorized changes and that thecopies are run in a controlled environment. A secure library is a repository of EUC programs that have been tested, validated, and approved by the appropriate authority. Executing copies of EUC programs out of a secure library can also help with version control, backup, and recovery of EUC programs. Having an independent party review the source calculations, implementing complex password controls, and verifying EUC results through manual calculations are not as effective as executing copies of EUC programs out of a secure library, as they do not prevent or detect unintentional modifications of complex calculations in EUC. References: End-User Computing (EUC) Risks: A Comprehensive Guide, End User Computing (EUC) Risk Management

NEW QUESTION: 226
□□ □ □□ □□ □□(CSA)□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□ □□ □□□□.
B. □□ □□□ □□□ □□ □□□ □□□ □□
C. □□ □□ □□□□ □□□ □□ □□□□ □□□□□.
D. □□ □□ □□□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 227
□□ □□□ □□□□ □□ IS □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□. □□□□ □□ □□□ □□□ □□□ □□□.
A. □□□ □□□ □□ □□□ □□□□□.
B. □□ □□□□ □□□ □□□ □□□□□.
C. □□ □□□□ □□□ □□□ □□□□□.

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

NEW QUESTION: 228
□□ □ □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□□ □□□ □□□□ □□ □□□ □□□□□.
D. □□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 229
□□ □ □□ □ □□□ □□□□ □□□ □□ □□ □ □□ □□□ □□□ □□ □□□□□ □□ □□□□□?
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: 230
□□ 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: 231

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

A. □□□ □□□□ □□

B. □□ □□ □□ □□
C. □□□ □□ □□
D. □□ □□ □□
Answer: (SHOW ANSWER)
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: 232
□□ □□ □□ IS □□□□ □□□□ □□□ □□□□□ □□□□ □□□ □ □□ □□□ □□ □□□ □□□□ □□□□ □□ □□□□□□. □□ □ IS □□□□ □□ □ □□ □□ □ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□ □□□ □□□□□.
B. □□ □□ □□□ □□ □□ □□□□□.
C. □□□□ □□ □□□ □□ □□ □□□□□ □□□□□□□.
D. □□ □□□□□ □□ □□□ □□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 233
IS □□□□ □□ □□□ □□, □□ □ □□ □□□□□ □□□ □ □□ □□□□ □ □□□ □□□□□?
A. □□□ □□□□ □□□ □□ □□ □□□ □□ □□□ □□ □□□□□.
B. □□ □ □□□ □□ □□□ □□□□ □□□□□.
C. □□□ □ □□ □□□ □□□ □□□□.
D. □□□ □□□ □□□□□ □□□□ □□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 234
□□ □□ IS □□□□ □□ □□□□ □□□□ □□□ □□ □ □□□□□□ □□□□ □ □ □□□□□□□ □□□□ □□□□ □ □□□ □□ □□□□□□. □□ □ □□□□ □ □ □□□□ □□□□ □□ □□ □□□□ □□ □□□□□?
A. □□ □□ □□□(IDS)□ □□□□□.
B. □□ □□□ □□□ □□□□□□□.

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

NEW QUESTION: 235
□□ □ □□□ □□□□□□ □□□ □□□□ □□ □□ □□□ □□□□ □ □□ □□□ □□ □□ □□□□□?
A. □□□□ □□□□□ □□□□
B. □□□□ □□□□ □□□□□
C. □□□ □□ □□ □□□
D. □□□ □□ □□□□□ □□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 236
□□□ □□ □□ □□□ □□□ □ IS □□□□ □□□ □□ □□□ □□□□ □□□□□ □ □□□□ □□□.
A. □□ □□ □□□□.
B. □□ □□ □□□□□.
C. □□ □□ □□ □□.
D. □□ □□ □□.
Answer: A (LEAVE A REPLY)
Information security policies are high-level statements that define the organization's approach to protecting its information assets from threats and risks. They should be based primarily on a risk management process, which is a systematic method of identifying, analyzing, evaluating, treating, and monitoring information security risks. A risk management process can help ensure that the policies are aligned with the organization's risk appetite, business objectives, legal and regulatory requirements, and stakeholder expectations. An information security framework is a set of standards, guidelines, and best practices that provide a structure for implementing information security policies. It can support the risk management process, but it is not the primary basis for defining the policies. Past information security incidents and industry best practices can also provide valuable inputs for defining the policies, but they are not sufficient to address the organization's specific context and needs. References: Insights and Expertise, CISA Review Manual (Digital Version)

NEW QUESTION: 237
IS □□□□ □□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□ □□ □□ □□ □ □□□ □□□□□?
A. □□ □□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□□ □□□□□.
C. □□□□ □□ □□□ □□□□□.

D. □□□ □□ □□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

The primary reason an IS auditor should discuss observations with management before delivering a final report is A. Validate the audit observations. This is because discussing the observations with management can help the auditor to ensure that the findings are accurate, complete, and supported by sufficient evidence1. It can also help the auditor to obtain management's perspective and feedback on the issues and risks identified, and to avoid any misunderstandings or surprises when the final report is issued2.

NEW QUESTION: 238

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

A. □□ □□□ □□□□□ □□□□□.

B. □□□□□ □□□□ □□ SIEM □□□□ □□□ □□□□□.

C. □□ □□□ □□□ □□ □□ □□□ □□□ □□

D. □□□□□ □□□□ □□□□□□ □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 239

□□ □□ □□ □□□□□ □□□□ 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: 240

□□□□□ □□ □□ □□(KPI)□ □□□ □□□ □□□.

A. □□□□ □□□ □□□ □□□.

B. □□□□ □□ □□□□□.

C. □□ □□□ □□□□ □□ □□ □□□□□.

D. □□ □□ □□□□.

Answer: (SHOW ANSWER)

A key performance indicator (KPI) is a quantifiable measure of performance over time for a specific objective1. KPIs help organizations and teams track their progress and achievements towards their strategic goals. To be useful, a KPI must have a target value, which is the desired level of performance or outcome that the organization or team aims to achieve. A target value provides a clear direction and a benchmark for measuring success or failure. Without a target value, a KPI is meaningless, as it does not indicate whether the performance is good or bad, or how far or close the organization or team is from reaching their objective.

NEW QUESTION: 241

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

A. □□□□□ □□□□ □□ □□□ □□□□□□

B. □□□ □□□□□ □□ □□ □□ □□ □□

C. □□□ □□□□ □□□□□ □□□□□.

D. □□ □□□□□□ □□□□□□□ □□□□□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 242

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

A. □□ □□ □□□ □□ □□□□□ □□□□ □□

B. □□ □□□ □□ □□ □□□ □□□ □□

C. □□□□ □□ □□□ □□□□□ □□ □□□ □□□□□.

D. □□□□ □□ □□□ □□□□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

Sending a copy of the transaction logs to offsite storage on a daily basis would minimize the risk of losing transactions as a result of a disaster. This is because offsite storage provides a backup of the data that can be recovered in case of a catastrophic event that destroys or damages the onsite data. Storing a copy of the transaction logs onsite in a fireproof vault (B) would not protect the data from other types of disasters, such as floods, earthquakes, or theft. Encrypting or signing (D) a copy of the transaction logs and storing them on a local server would not prevent the loss of data if the server is affected by the

disaster. Encryption and digital signatures are security measures that protect the confidentiality and integrity of the data, but not the availability.
Reference: CISA - Certified Information Systems Auditor Study Guide1, Chapter 5: Protection of Information Assets, Section 5.2: Backup and Recovery Concepts, Page 353.

NEW QUESTION: 243
□□ □□□□ □□□ □□□□□□□ □□□□ □□□ □ IS □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□□□□ □□□
B. □□ □□
C. □□□ □□ □□
D. □□ □□□ □□
Answer: C (LEAVE A REPLY)
The most important thing for an IS auditor to review when evaluating the accuracy of a spreadsheet that contains several macros is the formulas within macros. Macros are sequences of commands or instructions that can automate tasks or calculations in a spreadsheet. Formulas are expressions that perform calculations on values or data in a spreadsheet. The accuracy of a spreadsheet depends largely on whether the formulas within macros are correct, consistent, and complete. The IS auditor should review the formulas within macros to verify that they produce the expected results and do not contain any errors or inconsistencies. The other options are not as important as formulas within macros, as they do not directly affect the accuracy of a spreadsheet. Encryption of the spreadsheet is a security control that can protect the confidentiality and integrity of the spreadsheet, but it does not ensure its accuracy. Version history is a document control feature that can track and manage changes to the spreadsheet, but it does not verify its accuracy. Reconciliation of key calculations is a validation technique that can compare and confirm the results of calculations with other sources, but it does not evaluate the accuracy of formulas within macros. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.2

NEW QUESTION: 244
□□ □ □□□(PKI) □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□□ □□□□ □□□□ □□ □□ □□ □□□□□□
B. □□□□(CA)□□ □□□ □□□□ □□□□
C. □□□□□□ □ □□ □□□□ □□□□
D. □□□□ □□□□ □□□□ □□□□ □□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 245
□□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□ □ □□□□□?
A. □□ □□□ □□□ □□

B. □□ □□ □□
C. □□ □□ □□□ □□□□□ □□□ □□□□□□□.
D. □□ □ □□ □□ □□
Answer: D (LEAVE A REPLY)
The most important responsibility of user departments associated with program changes is approving changes before implementation. This is because user departments are the primary stakeholders and beneficiaries of the program changes, and they need to ensure that the changes meet their requirements, expectations, and objectives. User departments also need to approve the changes before implementation to avoid unauthorized, unnecessary, or erroneous changes that could affect the functionality, performance, or security of the program.
Providing unit test data is a responsibility of user departments associated with program changes, but it is not the most important one. Unit test data is used to verify that the individual components of the program work as expected after the changes. However, unit test data alone cannot guarantee that the program as a whole works correctly, or that the changes are aligned with the user departments' needs.
Analyzing change requests is a responsibility of user departments associated with program changes, but it is not the most important one. Analyzing change requests is the process of evaluating the feasibility, necessity, and impact of the proposed changes. However, analyzing change requests does not ensure that the changes are implemented correctly, or that they are acceptable to the user departments.
Updating documentation to reflect latest changes is a responsibility of user departments associated with program changes, but it is not the most important one. Updating documentation is the process of maintaining accurate and complete records of the program's specifications, features, and functionsafter the changes.
However, updating documentation does not ensure that the changes are effective, or that they are approved by the user departments.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 281
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

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

NEW QUESTION: 247
□□ □□□□□ □□□ □□□□ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □□ □ □□□□□□.
IS □□□□ □□□ □□ □□□ □□□□ □□□.
A. □□□ □□□□ □□ □□□□ □□□□.
B. □□□□□ □□□ □□□□ □□□ □□□ □□□□ □□□□□ □□□□.
C. □□□ □□ □□□ □□□□ □□□□□.
D. □□ □□□ □□□□□ □□□□ □□ □□ □□□□ □□□□ □□□ □□□□□ □□ □□.
Answer: B (LEAVE A REPLY)
An IS auditor should be concerned because deleting the files logically does not overwrite the files' physical data. Deleting a file from a hard disk only removes the reference or pointer to the file from the file system, but does not erase the actual data stored on the disk sectors. The deleted data can still be recovered using special tools or techniques until it is overwritten by new data. This poses a risk of data leakage, theft, or misuse if the hard disk falls into the wrong hands. To securely dispose of a system containing sensitive data, the hard disk should be wiped or sanitized using methods that overwrite or destroy the physical data beyond recovery. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 248
IS □□□□ □□□□ □□□□ □□□□ □□□□ □ □□ □ □□□□ □□□ □□□ □ □ □□□ □□□□□ □□□ □□ □□□. □□□□ □□ □□□ □□□ □□□□.
A. □□ □□□□ □□□□ □□□□□.
B. □□□ □□ □□□ □□□□□ □□□□□.
C. □ □□□□ □□□□□.
D. □□ □□□□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
□□□ IT □□ □□ □□□□ □□□□ □□□ □□□ □ IS □□□□ □□ □□□ □□□ □ □□□ □□□□□?
A. □□ □□ □□(MFA)□ □□ □□□ □□□ □□□□□□ □□
B. □□□□ □□□□□□ □□
C. □□ □□ □□□ □□□□□□ □□
D. □□□□ □□□□ □□ □□ □□□□□ □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 250
□□ □ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?

A. □□ □□ □□□ □□ □□ □□ □□(RPO)□ □□□□□
B. □□ □□ □ □□□ □□□ □□□ □□□□ □□
C. □□ □ □□□ □□□ □□ □□□□ □□□ □□□□□□.
D. IT □□□□ □□□ □□□ □□ □□□ □□□□ □□□□□.
Answer: B (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 business' established protocol for maintaining information, typically defining what data needs to be retained, the format in which it should be kept, how long it should be stored for, whether it should eventually be archived or deleted, who has the authority to dispose of it, and what procedure to follow in the event of a policy violation1. A data retention policy can help an organization to:
Comply with legal and regulatory requirements that mandate the retention and disposal of certain types of data, such as financial records, health records, or personal data Reduce the risk of data breaches, theft, loss, or corruption by minimizing the amount of data stored and ensuring proper security measures are in place Save costs and resources by optimizing the use of storage space and reducing the need for backup and recovery operations Enhance operational efficiency and performance by eliminating unnecessary or outdated data and improving data quality and accessibility Support business continuity and disaster recovery plans by ensuring critical data is available and recoverable in case of an emergency Facilitate audit trails and investigations by providing evidence of data authenticity, integrity, and provenance Therefore, by implementing a data retention policy, an organization can limit its liability associated with storing and protecting information, as well as improve its data governance and management practices.
References:
Data Retention Policy 101: Best Practices, Examples & More

NEW QUESTION: 251
□□ □ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
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: 252
□□ □□□ □□ □□□ □□□ □□□□.
A. □□□□□ □□□□ □□□□□.
B. □□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□□ □□□□ □□□□□.
D. □□ □□□□ □□□□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 253
□□ □ □□□□ □□□□□□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□□□ □ □□ □□□ □□ □□ □□□ □□□□□?
A. □□ □ □□□ □□ □□
B. □□ □ □□□ □□ □□□
C. □□ □ □□□ □□ □□□ count □□ □□ □ □□
D. □□ □ □□□ □□□ □□ □□□ □□□ □□□
Answer: A (LEAVE A REPLY)
Hashing is a technique that transforms data into a fixed-length value, called a hash or a digest, that uniquely represents the original data. Hashing can be used to validate the integrity of data communicated between production databases and a big data analytics system by comparing the hash values of the data before and after the communication. If the hash values match, the data has not been altered; if they differ, the data has been tampered with or corrupted. Hashing is a better security control than encrypting, running and comparing the count function, or hosting a digital certificate for this purpose because:
Encrypting in-scope data sets can protect the confidentiality of the data, but not necessarily the integrity.
Encryption algorithms can be broken or bypassed by malicious actors, or encryption keys can be compromised or lost. Moreover, encryption adds overhead to the communication process and may affect the performance of the big data analytics system.
Running and comparing the count function within the in-scope data sets can only verify the number of records or elements in the data sets, but not the content or quality of the data. The count function cannot detect any changes or errors in the data values, such as missing, duplicated, corrupted, or manipulated data.
Hosting a digital certificate for in-scope data sets can provide authentication and non-repudiation for the data sources, but not integrity for the data itself. A digital certificate is a document that contains information about the identity and public key of an entity, such as a

person, organization, or device. A digital certificate does not contain or verify the actual data that is communicated between production databases and a big data analytics system.
References:
Ensuring Data Integrity with Hash Codes
Database Security: An Essential Guide
Control methods of Database Security

NEW QUESTION: 254
□□ □ □□□ □□□ □□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□ □□□ □□□□ IT □□ □□
B. □□ □□□ IT □□□□□ □□□□ □□ □□□□□.
C. □□ □ □□ □□□ □□□ □□□ IT □□ □□
D. □□ □□□□□ □□□ IT □□ □□□ □□□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 255
□□□□ □□ □□ □□□ □□□ □, □□ □ □□ □□□ □□ □ □□□□ □□□?
A. □□□□ □□□□ □□□□.
B. □□□□ □□ □□□□□□ □□□□ □□ □□□□.
C. □□□ □□ □□□ □□□□□□ □□□□□.
D. □□ □□ □□□ □□□□□ □□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256
IT □□□ □□ □□ □□□ □□□ □□□ □, IS □□ □□□□ □□ □ □□ □□□ □□ □□ □□□?
A. □□□□ □□ □□
B. □□ □□ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)
Risk management techniques should be included in an IS development methodology. An IS development methodology is a set of guidelines, standards, and procedures that provide a structured and consistent approach to developinginformation systems. A good IS development methodology should cover all the phases of the system development life cycle (SDLC), from planning and analysis to design, implementation, testing, and maintenance1.
Risk management techniques are an essential part of an IS development methodology, as they help to identify, assess, prioritize, mitigate, monitor, and communicate the risks that may affect the success of the system development project. Risk management techniques can also help to ensure that the system meets the requirements and expectations of the

stakeholders, complies with the relevant laws and regulations, and delivers value to the organization2.
The other options are not as relevant or appropriate as risk management techniques for an IS development methodology. Value-added activity analysis is a technique for evaluating the efficiency and effectiveness of business processes, but it is not specific to IS development3. Access control rules are policies and mechanisms for restricting or granting access to information systems and resources, but they are more related to security management than IS development4. Incident management techniques are methods for handling and resolving incidents that disrupt the normal operation of information systems and services, but they are more related to service management than IS development5.
References:
ISACA, CISA Review Manual, 27th Edition, 2019, p. 1911
ISACA, CISA Review Manual, 27th Edition, 2019, p. 1942
Value-Added Activity Analysis3
Access Control Rules4
Incident Management Techniques5

NEW QUESTION: 257
□□ □ IS □□□ □□□□ □□ □□□ □□□□□?
A. □□ □□□□ □□□ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□ □□.
B. □□ □□□□ □□ □□ □□□□ □□ □□□ □□□ □□□□□.
C. □□ □□□□ IT □□□□□ □□□ □□□□□.
D. □□ □□□□ □□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 258
□□ □ □□ □□ □□□ □□□ □□□□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□□?
A. □□□ □□□ □□ □□ □□□
B. □□□ □□ □□□□ □□□ □□□ □□
C. □□□□ □□ □□ □□□ □□ □ □□

D. □□□ □□□ □□ □□ □□ □□

Answer: (SHOW ANSWER)

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: 259

□□ □ □□□ □□□ □□ □□□ □□□ □□□□□?

A. □□□ □□ □□□ □□ □□□ □□□ □□□□

B. □□□□□□ □ □□□ □□ □□

C. □□□□ □□□ □ □□□□ □□ □□□ □□□

D. □□□ □□ □□ □□□□ □□□ □□□ □□□□

Answer: B (LEAVE A REPLY)

The most important control for virtualized environments is hardening for the hypervisor and guest machines.

Hardening is the process of applying security measures and configurations to reduce the vulnerabilities and risks of a system or device. Hardening for the hypervisor and guest machines is essential for protecting the virtualized environments from attacks, as they are exposed to various threats from both the physical and virtual layers. Hardening for the hypervisor and guest machines involves the following steps:

* Applying the latest patches and updates for the hypervisor and guest operating systems, as well as the applications and drivers running on them.
* Configuring the firewall and network settings for the hypervisor and guest machines, to restrict and monitor the network traffic and prevent unauthorized access or communication.
* Disabling or removing any unnecessary or unused features, services, accounts, or ports on the hypervisor and guest machines, to minimize the attack surface and reduce the potential entry points for attackers.
* Enforcing strong authentication and authorization policies for the hypervisor and guest machines, to ensure that only authorized users or administrators can access or manage them.
* Encrypting the data and communication for the hypervisor and guest machines, to protect the confidentiality and integrity of the information stored or transmitted on them.

* Implementing logging and auditing mechanisms for the hypervisor and guest machines, to record and track any activities or events that occur on them, and enable detection and investigation of any incidents or anomalies.
Hardening for the hypervisor and guest machines can help prevent or mitigate common attacks on virtualized environments, such as:
* Hypervisor escape: An attack where a malicious guest machine breaks out of its isolated environment and gains access to the hypervisor or other guest machines.
* Hypervisor compromise: An attack where an attacker exploits a vulnerability or misconfiguration in the hypervisor to gain control over it or its resources.
* Guest compromise: An attack where an attacker exploits a vulnerability or misconfiguration in a guest machine to gain access to its data or applications.
* Guest impersonation: An attack where an attacker creates a fake or cloned guest machine to trick other guests or users into interacting with it.
* Guest denial-of-service: An attack where an attacker consumes or exhausts the resources of a guest machine to disrupt its availability or performance.
Therefore, hardening for the hypervisor and guest machines is the most important control for virtualized environments, as it can enhance their security, reliability, and performance.
For more information about hardening for virtualized environments, you can refer to some of these web sources:
* Hypervisor security on the Azure fleet
* Chapter 2: Hardening the Hyper-V host
* Plan for Hyper-V security in Windows Server

NEW QUESTION: 260
□□□□ □□□□ □□ □□□ □□□ □□ □□□□ □□□□□ □□□□□. □□ □□ □□□□ □□□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□□□□ □□ □□ □□□ □□□□□ □□□□□.
B. □□□ □□□ □□□ □□□ □□□□□.
C. □□ □ □□□□ □□□□ □□□□ □□□□□ □□□□□.
D. □□ □□ □□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The best recommendation to mitigate the risk of data leakage from lost or stolen devices that contain confidential data is to configure them to auto-wipe after multiple failed access attempts, as this would prevent unauthorized access and erase sensitive information from the device. Requiring employees to attend security awareness training, password protecting critical data files, or enabling device auto-lockfunction are also good practices, but they may not be sufficient oreffective in preventing data leakage from lost or stolen devices. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3

NEW QUESTION: 261

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

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: 262
IT □□ □□□ □□□ □ □□ □□ □□ □ □□ □□□□□?
A. □□□□ □□□ □□□□□.
B. □□□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The first step when conducting an IT risk assessment is to identify assets to be protected, which include hardware, software, data, processes, people, and facilities that support the business objectives and operations of an organization. Identifying assets to be protected helps to establish the scope and boundaries of the risk assessment, as well as the value and criticality of each asset. Identifying potential threats, assessing vulnerabilities, and evaluating controls in place are subsequent steps in the risk assessment process that depend on the identification of assets to be protected. References: CISA Review Manual (Digital Version), Chapter 2: Governance & Management of IT, Section 2.3: IT Risk Management

NEW QUESTION: 263
IS □□□□ □ □□ □□□ □□□□ □□□□. IS □□□□ □□ □□□ □□□ □□□□ □□□□.
A. □□ □□□□□ □□□□ □□□ □□ □□□□□.
B. □□ □□ □□□□ □□ □□□ □□□□□ □□□□□□□.
C. □□ □□□□□ □□□ □□□ □□ □□□□□.
D. □□ □□□□□ □□ 3□ □□□□□ □□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
The primary objective of an IS auditor when reviewing the installation of a new server is to ensure that security parameters are set in accordance with the organization's policies. Security parameters are settings or options that control the security level and behavior of the server, such as authentication methods, encryption algorithms, access rights, audit logs, firewall rules, or password policies7. The organization's policies are documents that define the security goals, requirements, standards, and guidelines for the organization's information systems. An IS auditor should verify that security parameters are set in accordance with the organization's policies to ensure that the new server complies with the organization's security expectations and regulations. The other options are less important or incorrect because:
* A. Security parameters should not be set in accordance with the manufacturer's standards alone, as they may not reflect the organization's specific security needs and environment. The manufacturer's standards are general recommendations or best practices for configuring the server's security parameters based on common scenarios and

threats. An IS auditor should compare the manufacturer's standards with the organization's policies and identify any gaps or conflicts that need to be resolved.
* B. A detailed business case should have been formally approved prior to the purchase of a new server rather than during its installation. A business case is a document that justifies the need for a new server based on its expected benefits, costs, risks, and alternatives. A business case should be approved by senior management before initiating a project to acquire a new server.
* D. The procurement project should have invited tenders from at least three different suppliers before purchasing a new server rather than during its installation. A tender is a formal offer or proposal to provide a product or service at a specified price and quality. Inviting tenders from multiple suppliers helps to ensure a fair and competitive procurement process that can result in the best value for money and quality for the organization.
References: Server Security - ISACA, [Information Security Policy - ISACA], [Server Hardening - ISACA], [Business Case - ISACA], [Tender - ISACA], [Procurement Management - ISACA]

NEW QUESTION: 264
□□ □ □□ □□ □□□□□ □□□ □□ □□□ □□ □□□□□?
A. □□ □□□ □□ □□□□ □□
B. □□ □□□ □□ □□□ □□
C. □□ □□□ IT □□□ □□
D. □□□□□ □□□□□ □□
Answer: A (LEAVE A REPLY)
The most critical factor for the success of an information security program is management's commitment to information security. Management's commitment to information security means that the senior management supports, sponsors, funds, monitors and enforces the information security program within the organization. Management's commitment to information security also demonstrates leadership, sets the tone and culture, and establishes the strategic direction and objectives for information security. User accountability for information security, alignment of information security with IT objectives, and integration of business and information security are also important factors for the success of an information security program, but they are not as critical as management'scommitment to information security, as they depend on or derive from it.
References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 265
□□ □ IS □□□□ □□□□□ □□ □□□□□ □□ □□□ □□□ □ □□ □□□□ □ □□ □□□□□?
A. □□□□ □□□ □□□□ □□ □□□ □□□□□.
B. □ □□□□□ □□ □ □□ □□ □□□ □□□□ □□

C. □□□ □□ □□□ □□ □□□ □□□□□.
D. □□□□ □□ □ □□□ □□□ □□□ □□□
Answer: C (LEAVE A REPLY)
User requirements are statements that describe what the users expect from the software system in terms of functionality, quality, and usability. They are essential inputs for the software development process, as they guide the design, implementation, testing, and deployment of the system. Therefore, an IS auditor's greatest concern when reviewing the early stages of a software development project would be the lack of acceptance criteria behind user requirements. Acceptance criteria are measurable conditions that define when a user requirement is met or satisfied. They help ensure that the user requirements are clear, complete, consistent, testable, and verifiable. Without acceptance criteria, it would be difficult to evaluate whether the system meets the user expectations and delivers value to the organization. Technical documentation, such as program code, is usually produced in later stages of the software development process. Completion of all requirements at the end of each sprint is not mandatory in agile software development methods, as long as there is a prioritized backlog of requirements that can be delivered incrementally. A detailed unit and system test plan is also important for ensuring software quality, but it depends on well-defined user requirements andacceptance criteria. References: Information Systems Acquisition, Development & Implementation, CISA ReviewManual (Digital Version)

NEW QUESTION: 266
□□ □ 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: 267

□□ □□ □□□□ □ □, □□□□ □□□ □□□ □□ IT □□□□ □□□ □ □□ □□□ □□ □□□ □□ □ □□ □□□□?

A. □□ □ □□□ □□□ □□□□□

B. □□□□□ □□ □ 1□□ □□

C. □□□ □□□ □□□□ □ □□ □□

D. □□□□ □□ □□□ □□ □□ □□

Answer: (SHOW ANSWER)

The best approach from a risk management perspective when implementing a large and complex data center IT infrastructure is to use a deployment plan based on sequenced phases, as this will allow the organization to break down the project into manageable and measurable stages, and to monitor and control the progress, quality, and outcomes of each phase12. A phased deployment plan can also help to reduce the risks of errors, failures, or disruptions that could affect the entire infrastructure, and to implement corrective actions or contingency plans as needed34.

References

1: Data Center Project Planning: A Guide to Success2 2: Data Center Project Planning: A Guide to Success4 3: Data Center Migration: A Step-by-Step Guide3 4: Data Center Migration: A Step-by-Step Guide1

NEW QUESTION: 268

□□ □ □□ □□(QA) □□□ □□□□ □ □□ □ □□□ □ □ □□ □□ □□□ □□□ □□?

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

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

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

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

Answer: A (LEAVE A REPLY)

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: 269
□□ □ □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□ □□□□□ □□□□ □ □□ □□□□□?
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: 270

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

A. □□ □□ □□(RPO)

B. □□ □□□ □□ □□ □□ □□(MAD)

C. □□ □□ □□(MTTR)

D. □□ □□ □□(KPIs)

Answer: B (LEAVE A REPLY)

The primary factor to determine system criticality is the maximum allowable downtime (MAD), which is the maximum period of time that a system can be unavailable before causing significant damage or risk to the organization. The MAD reflects the business impact and the recovery requirements of the system, and it can be used to prioritize the systems and allocate the resources for disaster recovery planning. The other options are not as important as the MAD, and they may vary depending on the system characteristics and the recovery strategy. The recovery point objective (RPO) is the maximum amount of data loss that is acceptable for a system. The mean time to restore (MTTR) is the average time required to restore a system after a failure. The key performance indicators (KPIs) are metrics that measure the performance and effectiveness of a system. References: CISA Review Manual (Digital Version) 1, page 468-469.

NEW QUESTION: 271

□□□ □□□□ □□ SaaS(Software as a Service) □□□ □□□□ □□□□ □□□□ □ □ □ □□□□□ □□□□□. □□ □ □□□ □□ □ □□□ □□□□ □□□ □□ □ □□□ □□□□□?

A. □□ □□□ □□□□□ □□□ □□□ □□ □ □□□□.

B. □□□□□ □□□ □□□□ □□□□ □□ □ □□□□.

C. □□□□□ □□ □□ □□(RTO) □□ □□□ □□ □□□□ □□□□ □□ □ □□□ □.

D. □□ □□□ □□□□□ □□□ □□□ □□□ □ □□□□.

Answer: (SHOW ANSWER)

An organization relies on an external vendor that uses a cloud-based Software as a Service (SaaS) model to back up its data. SaaS is a model in which the software is centrally hosted and accessed by the user via a web browser using the internet1. The vendor owns and maintains the software and the data, and the organization pays for the use of the service on a subscription or usage basis1. The greatest risk to the organization related to data backup and retrieval is that the vendor may be unable to restore critical data.

Data backup and retrieval are essential processes for ensuring the availability, integrity, and security of data in case of loss, corruption, or damage2. Data backup is the process of creating and storing copies of data in a separate location from the original data2. Data retrieval is the process of accessing and restoring the backed- up data when needed2.

Critical data are data that are vital for the operation, continuity, and recovery of the organization3.
If the vendor is unable to restore critical data, the organization may face severe consequences, such as:
Business disruption: The organization may not be able to perform its core functions, deliver its products or services, or meet its customer or stakeholder expectations3.
Revenue loss: The organization may lose income, market share, or competitive advantage due to reduced sales, customer dissatisfaction, or reputation damage3.
Legal liability: The organization may face lawsuits, fines, or penalties for breaching contractual, regulatory, or statutory obligations related to data protection, privacy, or security3.
Recovery cost: The organization may incur additional expenses for repairing or replacing the lost or corrupted data, restoring the system functionality, or compensating the affected parties3.
The other options are not as great as the vendor's inability to restore critical data. The organization may be locked into an unfavorable contract with the vendor, which may limit its flexibility, control, or choice over the service quality, cost, or duration4. However, this risk can be mitigated by negotiating better terms and conditions, reviewing the contract periodically, or switching to another vendor if possible4. The vendor may be unable to restore data by recovery time objective (RTO) requirements, which are the maximum acceptable time frames for restoring data after a disruption5. However, this risk can be reduced by setting realistic and achievable RTOs, monitoring the vendor's performance, or implementing alternative recovery strategies if needed5. The organization may not be allowed to inspect the vendor's data center, which may limit its visibility, transparency, or assurance over the service provider's infrastructure, security, or compliance.
However, this risk can be overcome by requesting third-party audits, certifications, or reports from the vendor that demonstrate their adherence to industry standards and best practices. Therefore, option B is the correct answer.
References:
What is SaaS? Software as a Service | Microsoft Azure
What is Data Backup? - Definition from Techopedia
Critical Data Definition
The Risks of Cloud Computing | Cloud Academy
Recovery Time Objective (RTO) Definition
[Cloud Computing Security Risks: What You Need To Know | CloudHealth by VMware]

NEW QUESTION: 272
□□ □ IS □□□□ □□ □□□□□ □□ □□□□ □□ □□□□ □□ □ □□ □□□□ □?
A. □□□□ □□□ □□□ □□□□ □□□□□□.
B. □□ □□□□□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Ensuring that the facts presented in the report are correct is the most important thing for an IS auditor to do during an exit meeting with an auditee. An IS auditor should confirm that the audit findings and observations are accurate, complete, and supported by sufficient evidence, as well as that the auditee understands and agrees with them. This will help to avoid any misunderstandings or disputes later on, as well as to enhance the credibility and quality of the audit report. The other options are less important things for an IS auditor to do during an exit meeting, as they may involve communicating the recommendations to senior management, specifying implementation dates for the recommendations, or requesting input in determining corrective action. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.5.21
* CISA Review Questions, Answers & Explanations Database, Question ID 222

NEW QUESTION: 273
□□□□□ □□□ □□ □□□ □□□ □□□□ □□ □ □□□ □□□ □□□□.
A. □□□□ □□ □□□ □□□□□□.
B. □□□ □□□ □ □□□ □□□ □□□ □□□□.
C. □□□□□ □□□□□ □□□□ □□□.
D. □□ □□(QA) □□□□ □□□ □□
Answer: (SHOW ANSWER)
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: 274

□□ □□□ IS □□□□ □□ □□□ □□□□ □□ □□ □ □□□ □□□ □□□□□. □ □ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□□ □□□□□.
B. □□ □□□□□ □□ □□□□ □□□□□ □□□□□.
C. □□□□□ 10% □□ □□ □□□ □□ □□□□□ □□□□ □□□□□.
D. □□ □□□ □□□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Ifmeasurable benefitswerenot defined, the organizationcannot assess whether the system achieved its intended goals, making it the mostcriticalissue.
* Measurable Benefits Not Defined (Correct Answer - D)
* No clear KPIs or success metricsmeans no way toevaluate ROI.
* Example:A company implementsan ERP systembut has no performance indicators to measure success.
* No Lessons Learned (Incorrect - A)
* Important but doesnot impact system effectiveness.
* Missing Dashboard Deliverables (Incorrect - B)
* A reporting issue,not a strategic failure.
* Budget Overrun (Incorrect - C)
* A financial concern butnot as critical as system success measurement.
References:
* ISACA CISA Review Manual
* COBIT 2019 (Project Governance)

NEW QUESTION: 275
□□ □ □□□ □□ □□□□□ □□□ □□□ □□□□ IS □□□□□ □□ □ □□□□ □ □□ □□ □□□□□?
A. □□□□ □□□ □□ □□□ □□ □□□□.
B. □□□ □□ □□□ □□ □□ □□□□□.
C. □□ □□ □□□ □□□□ □□□□□.
D. □□□ □□□ □□ □□□ □ □□ □□ □□ □□□ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 276
□□ □ IS □□□□ □□ □□□ □□ □□ □□ □□□ □□□ □ □□ □□ □□□□ □□ □□ □□□□□?
A. □□ □ □□ □□ □□ □□
B. □□ □□
C. □□□ □□
D. □□□ □□ □ □□
Answer: D (LEAVE A REPLY)

The organizational policies and procedures are the first source of guidance for an IS auditor when planning a customer data privacy audit. They provide the framework and objectives for ensuring compliance with legal and regulatory requirements, customer agreements and data classification. The IS auditor should review them first to understand the scope, roles and responsibilities, standards and controls related to customer data privacy in the organization. The other options are also important, but they are secondary sources of information thatshould be reviewed after the organizational policies and procedures. References: CISA Review Manual (Digital Version) 1, Chapter 2: Governance and Management of Information Technology, Section 2.5: Privacy Principles and Policies.

NEW QUESTION: 277

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

A. □□ □□□ □□□□ □□□ □□□□□□□ □□□□□.

B. □□□□ □□□ □□□□ □□ □□ □□

C. □□□□ □□□ □□ □□□ □□□□□□□.

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

Answer: C (LEAVE A REPLY)

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: 278
□□ □□□ □□□□ 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: 279
□□□□ □□□ □□ □□□(CASB)□ □□ □□□ □□□□ □□□□□□□□ □□□ (SaaS)□ □□□ □□□□ □□□□□. □□□ □□□ □□□ □ IS □□□□ □□□□ □ □ □□ □□□ □□□ □□□□□?
A. CASB□ SaaS □□□□□□□□ □□□□ □□ □□□□ □□□□ □□ □□ □□□□ □□□□□.
B. CASB□ □□□ □□□ □□□ □□□□ □□□□ □□□ □□□ □□□ □ □□□□□.
C. CASB□ □□□□ □□□□ □□ □□□ □□ □□□□ □□□ □□□ □□□□□.

D. CASB□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□ □□□ □□□ □□ □□□.

Answer: (SHOW ANSWER)

NEW QUESTION: 280

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: 281

□□ □ □□□ □□ □□ □ □□□ □□(SIEM) □□□□ □□ □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□□?

A. □□ □□ □□□

B. □□ □□ □□ □□□

C. □□□ □□□

D. □□ □□□

Answer: C (LEAVE A REPLY)

Substantive testing provides the best evidence of the validity and integrity of logs in an organization's security information and event management (SIEM) system, because it is a type of audit testing that directly examines the accuracy, completeness, and reliability of the data and transactions recorded in the logs. Substantive testing can involve various methods, such as re-performance, inspection, observation, inquiry, or computer-assisted audit techniques (CAATs), to verify the existence, occurrence, valuation, ownership, presentation, and disclosure of the log data1. Substantive testing canalso detect any

errors, omissions, alterations, or manipulations of the log data that may indicate fraud or misstatement2.
Compliance testing (A) is not the best evidence of the validity and integrity of logs in an organization's SIEM system, because it is a type of audit testing that evaluates the design and effectiveness of the internal controls that are implemented to ensure compliance with laws, regulations, policies, and procedures. Compliance testing can involve various methods, such as walkthroughs, questionnaires, checklists, or flowcharts, to assess the adequacy, consistency, and operation of the internal controls1. Compliance testing can provide assurance that the log data are generated and processed in accordance with the established rules and standards, but it does not directly verify the accuracy and reliability of the log data itself2.
Stop-or-go sampling (B) is not a type of audit testing, but a type of sampling technique that auditors use to select a sample from a population for testing. Stop-or-go sampling is a sequential sampling technique that allows auditors to stop testing before reaching the predetermined sample size if the results are satisfactory or conclusive. Stop-or-go sampling can reduce the audit cost and time by avoiding unnecessary testing, but it can also increase the sampling risk and uncertainty by relying on a smaller sample3. Stop-or-go sampling does not provide any evidence of the validity and integrity of logs in an organization's SIEM system by itself; it depends on the type and quality of the audit tests performed on the selected sample.
Variable sampling (D) is not a type of audit testing, but a type of sampling technique that auditors use to estimate a numerical characteristic of a population for testing. Variable sampling is a statistical sampling technique that allows auditors to measure the amount or rate of error or deviation in a population by using quantitative methods. Variable sampling can provide precise and objective results by using mathematical formulas and confidence intervals4. Variable sampling does not provide any evidence of the validity and integrity of logs in an organization's SIEM system by itself; it depends on the type and quality of the audit tests performed on the selected sample.
References:
Audit Testing Procedures - 5 Types and Their Use Cases
5 Types of Testing Methods Used During Audit Procedures | I.S. Partners Stop-or-Go Sampling Definition Variable Sampling Definition

NEW QUESTION: 282
□□ □□□□□ □□□ □□□ □□□□ □□□ □□□ □□, □□, □□ □□□ □□□□ □□ □□ □□□□ □□□□. IS □□□□ □□□ □□□ □□□ □ □□ □□□ □□ □□ □□□ □□□ □□ □□□ □□□□□. □□ □ □□ □□□□ □□ □□□ □□ □□□□?
A. □□□□ □□ □□□ □□
B. □□ □□ □□ □□ □□□□□ □□
C. □□ □ □□ □□□ □□□□□ □□□ □□
D. □□ □ □□ □□□□ 2□□ □□ □□

Answer: C (LEAVE A REPLY)
A monitored mantrap at entrance and exit points would be the most effective compensating control in this scenario. A mantrap is a physical security access control system comprising a small space having two sets of interlocking doors such that the first set of doors must close before the second set opens. By implementing a monitored mantrap, unauthorized access can be prevented and it can ensure that all individuals are logged when they enter and exit the server room12.
References: ISACA's Information Systems Auditor Study Materials3

NEW QUESTION: 283
□□ □ □□□ □□□ □□ □□□□□ □□□□ □□ □□□ □□□□?
A. □□□□□ □□□ □□□□□ □□□□ □□□□□□ □□
B. □□ □□ □□ □□□□□ □□□□ □□□□ □□
C. □□□□□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□
D. □□ □□ □□ □□□ □□ □□□□ □□
Answer: D (LEAVE A REPLY)
A top-down maturity model process is a method of assessing and improving the maturity level of a process or a set of processes within an organization. A maturity level is a measure of how well-defined, controlled, measured, and optimized a process is. A top-down maturity model process starts with defining the desired maturity level and then identifying the gaps and improvement opportunities for each process. This helps prioritize the processes that need the most attention and improvement. Therefore, a result of utilizing a top- down maturity model process is identification of processes with the most improvement opportunities.
A means of benchmarking the effectiveness of similar processes with peers, a means of comparing the effectiveness of other processes within the enterprise, and identification of older, more established processes to ensure timely review are not results of utilizing a top-down maturity model process. These are possible benefits or objectives of using other types of maturity models or assessment methods, but they are not specific to a top-down approach.

NEW QUESTION: 284
□□□□ □□□ □□□ □□ □□□ □□□□□□. □□ □□ □□□ □□□ □□□ □□ □□ □□ □□□□.
A. □□ □□.
B. □□ □□(QA).
C. □□ □□.
D. □□□□ □□.
Answer: C (LEAVE A REPLY)
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: 285
IT □□□□□□ □□□□ □□ □□□ □□ □□ □ □□□ □□□□□?
A. □□ □□□□□ □□ □□□ □□ □□□ □□□.
B. IT □□ □□□ □□ □□ □□□ □□□□□.
C. □□ □□ □□□ □□□□□□□ □□□□□□□.
D. □□ □□□ □□ □□□□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
The necessary condition for effective risk management in IT governance is that risk evaluation is embedded in management processes. Risk evaluation is the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation should be integrated into the management processes of planning, implementing, monitoring, and reviewing the IT activities and resources. This will ensure that risk management is aligned with the business objectives, strategies, and values, and that risk responses are timely, appropriate, and effective. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & ExplanationsDatabase

NEW QUESTION: 286
□ □□□ □□ □□ □□□□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□ □□□ □□. □ □□□□ □□□□ □□ □□□□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□ □□ □□□ □□□□□.
B. □□□□ □□ □□
C. □□□□ □□□□ □□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The best way to prevent a chip-level security vulnerability from being exploited is to install vendor patches.
A chip-level security vulnerability is a flaw in the design or implementation of a processor thatallows an attacker to bypass the normal security mechanisms and access privileged information or execute malicious code. A vendor patch is a software update provided by the manufacturer of the processor that fixes or mitigates the vulnerability. Installing vendor patches can help to protect the system from known exploits and reduce the risk of data leakage or compromise.
Security awareness training, reviewing hardware vendor contracts, and reviewing security log incidents are not as effective as installing vendor patches for preventing a chip-level

security vulnerability from being exploited. Security awareness training is an educational program that teaches users about the importance of security and how to avoid common threats. Reviewing hardware vendor contracts is a legal process that evaluates the terms and conditions of the agreement between the organization and the processor supplier. Reviewing security log incidents is an analytical process that examines the records of security events and activities on the system. These methods may be useful for other security purposes, but they do not directly address the root cause of the chip-level vulnerability or prevent its exploitation. References: Protecting your device against chip-related security vulnerabilities, New 'Downfall' Flaw Exposes Valuable Data in Generations of Intel Chips

NEW QUESTION: 287
□□ IT □□□□ □□ □□□ □□□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□ □□□□□□□ □□□□□.
B. □□□□ □□ □□ □□□□ □□□□□.
C. □□□□ □□ □□□□ □□□□.
D. □□□□□ □□ □□□ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
The scanning will not degrade system performance. This is the most important consideration when establishing vulnerability scanning on critical IT infrastructure, because any degradation of system performance could affect the availability, reliability, and functionality of the IT services that depend on the infrastructure. Scanning during non-peak hours (A) could reduce the impact of scanning on system performance, but it does not guarantee that the scanning will not cause any degradation. Scanning followed by penetration testing (B) could provide more in-depth information about the vulnerabilities and their exploitability, but it does not address the potential impact of scanning on system performance. Scanning cost- effectiveness is a relevant factor for choosing a scanning service or tool, but it is not as important as ensuring that the scanning will not compromise the system performance.
Reference: CISA Vulnerability Scanning, Description.

NEW QUESTION: 288
□□ □ □□ □ □□□ □□□ □□ □□□ □□ □□ □□□ □□□□□?

A. □□□□
B. □□□□
C. □□□□□□(LTE)
D. □□□ □□(NFC)
Answer: D (LEAVE A REPLY)
The technology that has the smallest maximum range for data transmission between devices is near-field communication (NFC). NFC is a short-range wireless technology that enables two devices to communicate when they are in close proximity, usually within a few centimeters. NFC is commonly used for contactless payments, smart cards, and device pairing. According to the Bluetooth Technology Website1, the effective range of NFC is less than a meter, while the other technologies have much longer ranges. Wi-Fi can reach up to 100 meters indoors and 300 meters outdoors2. Bluetooth can reach up to 800 feet with Bluetooth 5.0 specification3. Long-term evolution (LTE) can reach up to several kilometers depending on the cell tower and the device4.
References:
* 5: What is Wi-Fi? - Definition from WhatIs.com
* 6: Understanding Bluetooth Range | Bluetooth Technology Website
* 7: What is Bluetooth Range? What You Need to Know
* 8: How far can LTE signals travel? - Quora

NEW QUESTION: 289
□□□ □□ □□□ □□□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□□ □□, □□ IS □□ □□ □□□ □□ □□□□□?
A. □□ □□ □□□□□□ □□ □ IT □□□□ □□□□ □□
B. □□ IS □□ □□ □ □□□□□□ □□ □□
C. □□□□□ □□ □□□ □□ □ □□□□□ □□
D. □□ □□□□ □□□□ □□ □□□□ □□ □□□□□□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 290
□□□ □□□□ □□ □□□□ □□□ □□□□ IS □□□□□ □□ □□□ □□□ □□□ □□?
A. □□□ □□ □□□ □□□ □□□□.
B. □□□ □□□□ □ □□□ □□ □□□ □□□□ □□□□□.
C. □□ □□□ □□ □□□□□ □□□□ □□□□.
D. □□□□ □□□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
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: 291
□□ □□ □□ 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: 292
□□□ □ □□□ □□□□ □□□□□ □□□□ □□ □□□ □□□ □□□□, □□ □ □ □ □□□ □□□□ □□ □□□ □□□?
A. □□ □□ □□□ □□ □□
B. □□□ □□□□□ □□□ □□□
C. □□□ □□□□□ □□
D. □□ □□□ □□□ □□□□□ □□
Answer: (SHOW ANSWER)
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: 293

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

A. □□□□ □□□□

B. □□□□ □□

C. □□□

D. □□□ □□

Answer: C (LEAVE A REPLY)

Materiality is the primary consideration when determining which issues to include in an audit report, as it reflects the significance or importance of the issues to the users of the report. Materiality is a relative concept that depends on the nature, context, and amount of the issues, as well as the expectations and needs of the users. Materiality helps the auditor to prioritize the issues and communicate them clearly and concisely.

References

ISACA CISA Review Manual, 27th Edition, page 256

Materiality in Auditing - AICPA

Materiality in Planning and Performing an Audit - IAASB

NEW QUESTION: 294

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

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: 295
IS □□□□ □□ □□□□ □□□□□□ □□□□ □□□ □□ □□, □□□ □□ □□ □ □ □ □□□ □□ □□ □□ □□□ □□□ □□□□□. □□□□ □□□ □□□ □□□ □ □□□ □□ □□ □□□□ □□ □□ □□ □ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 296
□□ □ □□□□□□ □□□□□ □□□□□(API) □□ □□□ □□□ □□ □□□ □□□ □ □□ IS □□□□ □□ □□ □□ □□ □□□ □□□□□?
A. SOAP(Simple Object Access Protocol)□ □□□□□.
B. API □□□□□□ □□□□□□.
C. □□ □□□ □□□ □□(XML) □□□ □□□□□□.
D. □□ □□ □□(TLS)□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 297
□□ □ □□□ □□ □□□ □□□ □□ □ □□□ □□□□□?
A. □□ □□□□□ □□□□ □□□ □ □□□□.
B. □□□□□ □□□ □□ □□□ □□□ □ □□□□.
C. □□□□ □□ □□□ □□□ □ □□□□.
D. □□□□ □□□ □□□ □□□□ □□ □□ □□□ □ □ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 298
□□ □ □□ □□□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □ □□□ □□ □□ □□□□ □□□ □ □ □□□□?
A. □□□ □□□ □□□□ □□□□ □□□□.
B. □□□ □□□ □□ □□□ □□□ □□□□ □□□□□□□.
C. □□□ □□□□ □□ □□□□ □□□□ □□□.
D. □□□ □□□ □□ □□□ □□□□ □□□□□.

Answer: D (LEAVE A REPLY)
Access to the data center is controlled by a mantrap provides the greatest assurance that only authorized individuals can access a data center. A mantrap is a physical security device that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens1. A mantrap prevents unauthorized entry by requiring authentication at both doors, such as biometric scanners, card readers, or PIN codes. A mantrap also prevents tailgating, which is the act of following an authorized person into a restricted area without proper authorization2. A mantrap can also detect and trap intruders who attempt to force their way through the doors.
The other options are less effective physical controls for data center access. The data center is patrolled by a security guard is a deterrent measure, but it does not prevent unauthorized access by itself. A security guard may not be able to monitor all entry points, or may be distracted, bribed, or overpowered by intruders. Access to the data center is monitored by video cameras is a detective measure, but it does not prevent unauthorized access either. Video cameras can record the activities of intruders, but they cannot stop them from entering or alert the security personnel in real time. ID badges must be displayed before access is granted is a preventive measure, but it relies on human verification, which can be prone to errors or manipulation. ID badges can also be lost, stolen, or forged by intruders.
References:
Mantrap (access control) - Wikipedia1
Tailgating (security) - Wikipedia2

NEW QUESTION: 299
IS □□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □□ □ □□ □□ □ □ □□□□ □□ □□ □□□ □□□ □□□□□?
A. □□ □□
B. □□□ □□
C. □□ □□ □□□
D. □□ □□
Answer: (SHOW ANSWER)
Risk appetite is the amount and type of risk that an organization is willing to accept in pursuit of its objectives. Risk appetite reflects the organization's risk culture, strategy, and tolerance, and guides the organization's risk management practices. The most useful information about risk appetite can be obtained from the risk policies, which are the documents that define the organization's risk management framework, principles, objectives, roles, responsibilities, and processes. Risk policies also establish the criteria and thresholds for identifying, assessing, prioritizing, mitigating, and monitoring risks, as well as the reporting and escalation mechanisms for risk issues. By reviewing the risk policies, an IS auditor can evaluate whether they are consistent, comprehensive, and

aligned with the organization's risk appetite and whether they provide clear guidance and direction for managing risks effectively.
The other options are not correct because they are either not the most useful or not relevant to risk appetite.
Risk assessments are the processes of identifying, analyzing, and evaluating the risks that may affect the organization's objectives. Risk assessments provide information about the current risk profile and exposure of the organization, but they do not indicate the organization's risk appetite or preferences. Prior audit reports are the documents that summarize the findings, recommendations, and conclusions of previous audits. Prior audit reports may provide information about the past performance and issues of the organization's risk management practices, but they do not reflect the organization's risk appetite or expectations. Management assertion is a statement or declaration made by management about the accuracy, completeness, validity, or reliability of a certain fact or data. Management assertion may provide information about the management's confidence or opinion on a specific risk or issue, but it does not represent the organization's risk appetite or criteria.

NEW QUESTION: 300
□ □□□ □□□□ IT □□□ □□□ □□□ □□□□ □□ □□□□ □□□□□ □□□□ □□□□□ □□□□□□. □□□□ □□ □□ □□ □□ □ IS □□□□□ □□ □ □□□ □ □□□□□?
A. □□ □□□ □□□ □□ □□□ □□□□□ □□ □□□ □□□□□□□.
B. □□ □□□ □□□□ □□□□ □□□ □□ □□□ □□□□□.
C. □□ □□□ □□□□□□□(CRO)□□ □□□□□.
D. □□ □□□ □ □□ □□ □□(KPI) □□
Answer: A (LEAVE A REPLY)
Disabling operational logging compromises critical functions such as security monitoring, troubleshooting, and compliance reporting. Logs are essential for tracking system activities, identifying anomalies, and conducting forensic investigations in case of incidents. Enhancing processing speed and saving storage should not come at the cost of reducing logging, as this increases security risks and weakens the organization's ability to detect and respond to threats.
* Adopting a Peer-Inspired Service Delivery Model (Option B):This might pose risks if not customized for the organization's context, but it is not as critical as the loss of operational logging.
* Delegating Business Decisions to the CRO (Option C):While unconventional, this does not inherently introduce risks to IT service delivery unless operational control issues arise.
* Eliminating Reports and KPIs (Option D):This could hinder performance tracking but does not compromise operational security as severely as disabling logging.
Operational logging is foundational to maintaining security, reliability, and accountability in IT environments.

Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 301
□□ □ □□□ □□□□□□ □□□□ □□□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□□
D. IT □□□ □□□□
Answer: (SHOW ANSWER)
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: 302
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: 303
□□□ □□ □□□□□ □□ □□□□□□ □□□ □□ CPU □□□ □□ □□□ □□□□ □□□□ □□□ □□□□□. □□ □ IS □□□□ IT □□□ □□ □□□□ □□ □□□□ □?
A. □□□□ □□□ □□ □ □□□ □□ □ □□ □□□ □□ □□□□□.
B. □□□ □□□ □□ □□□ □□□ □□□ □□□□ □ □□□□ □□□□□.
C. □□ □□ □ □□ □□□ □□□□ □□ □□□ □□ □□□□ □□□□.
D. □□ □□ □□□ □□ □□□ □ □□ □□ □□□□ □□ □□□□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 304
IS □□□□ □□□□□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□□ □ □□ □□□□□□. IS □□□□ □□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□ □□ □□□□ □□
B. □□ □□ □□□ □□□□□.
C. □□ □□□□ □□□□□.
D. □□ □□ □□
Answer: D (LEAVE A REPLY)
The best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities is to perform a configuration review. A configuration review is an audit procedure that involves examining and verifying the security settings and parameters of application servers against predefined standards or best practices. A configuration review can help to identify and remediate any deviations, inconsistencies, or misconfigurations thatmay expose the application servers to unauthorized access, exploitation, or compromise6. A configuration review can also help to ensure compliance with security policies and regulations, as well as enhance the performance and availability of application servers. The other options are less effective or incorrect because:
* A. Improving the change management process is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While improving the change management process may help to prevent future inconsistencies or misconfigurations in application server settings, it does not ensure that the existing ones are detected and corrected.
* B. Establishing security metrics is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While establishing security metrics may help to measure and monitor the security performance and posture of application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected.

* C. Performing a penetration test is not the best recommendation by the IS auditor for finding that application servers had inconsistent security settings leading to potential vulnerabilities, as it does not address the root cause of the problem or provide a specific solution. While performing a penetration test may help to simulate and evaluate the impact of an attack on application servers, it does not ensure that the existing inconsistencies or misconfigurations in application server settings are detected and corrected. References: Configuring system to useapplication server security - IBM, Application Security Risk: Assessment and Modeling - ISACA, Five Key Components of an Application SecurityProgram - ISACA, ISACA Practitioner Guidelines for Auditors - SSH, SCADA Cybersecurity Framework - ISACA

NEW QUESTION: 305
□□ □ □□□ □□ □□(DLP) □□□ □□□ □□□□ □□□ □□□□ □ □□ □□□□ □□ □□□□□?
A. □□□□ □□□ □□
B. □□ □□ □□
C. □□□ □□□□
D. □□ □□□
Answer: (SHOW ANSWER)
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: 306
□□ □ IS □□ □□□□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□ □?
A. □□ □□□□□ □□□□□ □□□□ IS □□ □□□ □□ □□□□ □□□ □□□□ □.
B. IS □□ □□□□ □□ □□□ □□ □□□ □□□ □□□□□.
C. IS □□ □□, □□ □ □□ □□□□ □□ □□□□□.
D. IS □□ □□ □□ □□ □□(QA)□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)

The best way to foster continuous improvement of IS audit processes and practices is to establish and embed quality assurance (QA) within the IS audit function, as this will ensure that the IS audit activities are aligned with the standards, expectations, and objectives of the organization and the stakeholders12. QA involves periodic internal and external assessments, benchmarking, feedback, and root cause analysis to identify and address gaps, issues, and opportunities for improvement34.
References
1: The Basics and Principles of Continuous Improvement4 2: ISO 9001 Auditing Practices Group Guidance on5 3: INSIGHTS TO QUALITY3 4: Continuous Auditing: Coordinating Continuous Auditing and Monitoring to Provide Continuous Assurance2

NEW QUESTION: 307
□□ □ □□ □□ □□ □□□□□ □□□□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□□□□□ □□□□ □□
B. □□□□□ □□□ □□□ □□
C. □□ □□ □□□□ □□ □□ □□ □□
D. □□□□ □□ □□ □□
Answer: (SHOW ANSWER)
The success rate of social engineering attacks directly measures the behavioral changes resulting from an information security awareness program. Employees who are aware and informed are better equipped to identify and thwart such attacks.
* Reduction in Reported Incidents (Option A):This may indicate underreporting rather than program effectiveness.
* Reduction in Cost of Maintaining the Program (Option C):This reflects cost efficiency, not program effectiveness.
* Reduction in Number of Attacks (Option D):The number of attacks is beyond the control of awareness programs and does not reflect their impact.
Reference:ISACA CISA Review Manual, Job Practice Area 4: Protection of Information Assets.

NEW QUESTION: 308
□□□ □□□ IS □□ □□ □□□□□□ □□ □□□□□ □□ □□ □□□ □ □ □□□ □□□ □□□□□□□. □□ □ IS □□□□ □□ □□ □□□ □□□□□?
A. □□□ □ □□ □ □□□□ □□ □□ □□□ □□□ □ □□□ □□□ ID □□ □□□ □□□□ □□□.
B. □□ □□□□ □□□ □□ □□□□ □□□□ □□ □□□□ □□□□□□ □ □□□ □□□ □□□ □□□.
C. □□□□□□ □□□□□□ □□□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□ □ □□□ □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 309
□□ □□ □□ □ IS □□□□ □□ □ □□ □□□ □□□□ □□ □□ □□□ □□□ □□ □□□?
A. □□□□ □□ □□□ □□□ □□□□ □□
B. □□ □□□□□ □□ □□ □□□ □□□□□.
C. □□□□ □□ □□□ □□□□ □□□□ □□ □□□ □□ □□□□□.
D. □□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
A post-incident review (PIR) is a process to review the incident information from occurrence to closure and to identify potential findings and recommendations for improvement1. The most important reason for an IS auditor to examine the results of a PIR is to evaluate the effectiveness of continuous improvement efforts and to ensure that the lessons learned from the incident are implemented and followed up2. A PIR can help an organization to eliminate or reduce the risk of the incident to re-occur, improve the initial incident detection time, identify improvements needed to diagnose and repair the incident, and update the incident management best practices1. Therefore, a PIR is a valuable source of information for an IS auditor to assess the maturity and performance of the organization's incident management process.

NEW QUESTION: 310
□□ □□□ □□□□□□□ □□□ □□□□ □□ □□ □□□ □□□ □□□□.
A. □□ □ □□□ □□□□□.
B. □□ □□□ □□□ □□□□□.
C. □□□ □□ □□□ □□□□□.
D. □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The best way to evaluate the effectiveness of a newly developed application is to review acceptance testing results. Acceptance testing is a process of verifying that the application meets the specified requirements and expectations of the users and stakeholders. Acceptance testing results can provide evidence of the functionality, usability, reliability, performance, security and quality of the application. Performing a post- implementation review, analyzing load testing results, and performing a secure code review are also important activities for evaluating an application, but they are not as comprehensive or conclusive as acceptance testing results.
References: Info Technology & Systems Resources | COBIT, Risk, Governance ... - ISACA, IT Governance and Process Maturity

NEW QUESTION: 311
□□ □□ □□□ □□□ □ IT □□□□ □□ □□ □□ □□(RPO)□ □□□ □□□□□□ □ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□ □ □□□ □□□□ □ □□ □□ □□□?

A. □□□
B. □□□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)
Mirroring (Option B) is the best choice for applications requiring a short Recovery Point Objective (RPO) because it provides real-time replication of data, ensuring minimal data loss.
ISACA CISA Reference: Data replication strategies in disaster recovery planning emphasize mirroring for high-availability systems.
Risk Implication: If mirroring is not implemented for critical systems, significant data loss may occur in the event of a failure.
Alternative Choices:
Option A: Snapshots capture data at specific points in time, leading to potential data loss.
Option C: Log shipping has delays due to batch processing.
Option D: Backups are periodic and not suitable for short RPO needs.

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

NEW QUESTION: 313
□□ □ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□ □□□□□.
B. □□□ □□ □□□ □□□ □□□□□.
C. □□□ □□ □□□□□ □□□.
D. □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 314
□□ □ □□ □□ □□□ □□ □□□□ □□□□ □ □□ □□□□□?
A. □□□ □□□ □□□□□ □□□ □□□□ □□
B. □□□ □□□□□ □□□
C. □□□ □□ □□□□ □□ □□
D. □□□ □□ □□ □□ □□□ □□
Answer: (SHOW ANSWER)

The most important thing to include in security awareness training is how to respond to various types of suspicious activity. Security awareness training is a program that educates employees about the importance of security and how to avoid common threats and risks. One of the main objectives of security awareness training is to enable employees to recognize and report any signs of malicious or unauthorized activity, such as phishing emails, malware infections, data breaches, or social engineering attempts. By teaching employees how to respond to various types of suspicious activity, security awareness training can help to prevent or mitigate the impact of security incidents, protect the organization's assets and reputation, and comply with legal and regulatory requirements.
The other options are not as important as option A. The importance of complex passwords is a useful topic, but not the most important thing to include in security awareness training. Complex passwords are passwords that are hard to guess or crack by using a combination of letters, numbers, symbols, and cases. Complex passwords can help to protect user accounts and data from unauthorized access, but they are not sufficient to prevent all types of security incidents. Moreover, complex passwords may be difficult to remember or manage by users, and may require additional measures such as password managers or multi-factor authentication.
Descriptions of the organization's security infrastructure is a technical topic, but not the most important thing to include in security awareness training. Security infrastructure is the set of hardware, software, policies, and procedures that provide the foundation for the organization's security posture and capabilities. Security infrastructure may include firewalls, antivirus software, encryption tools, access control systems, backup systems, etc. Descriptions of the organization's security infrastructure may be relevant for some employees who are involved in security operations or administration, but they may not be necessary or understandable for all employees who need security awareness training.
Contact information for the organization's security team is a practical detail, but not the most important thing to include in security awareness training. Security team is the group of people who are responsible for planning, implementing, monitoring, and improving the organization's security strategy and activities. Contact information for the organization's security team may be useful for employees who need to report or escalate a security issue or request a securityservice or support.
However, contact information for the organization's security team is not enough to ensure that employees know how to respond to various types of suspicious activity. References: Security Awareness Training | SANS Security Awareness, Security AwarenessTraining | KnowBe4, SecurityAwareness Training Course (ISC)² | Coursera

NEW QUESTION: 315
24/7 □□ □□□□ □□□□□□□□ □□□ □□□□ □□□ □□□ □□ □□ □□ □□ □□□□ □□□ □□□□. □□ □□ □□ □ □□ □□ □□□□□ □□□□ □□□ □□ □ □□□ □□ □ □□□ □ □□□□?
A. □□□□□□□ □□ □□□□ □□□ □□□ □□□□□□□ □□□□□.

B. □□□ □□□□□□ □□□ □□□□ □□
C. □□□□□□ □□□ □□□□□ □□□ □□ □□□ □□□□□.
D. □□□□ □□□ □□□□ □□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The best recommendation to address the risk of privileged application accounts with passwords set to never expire in a 24/7 processing environment is to introduce database access monitoring into the environment.
Database access monitoring is a security control that tracks and records all activities and transactions performed on a database, especially by privileged users or accounts. Database access monitoring can help address the risk of privileged application accounts with passwords set to never expire by detecting and alerting any unauthorized or abnormal access or actions on the database. The other options are not as effective as database access monitoring in addressing the risk, as they may cause disruption to the business or violate the access management policy. Modifying applications to no longer require direct access to the database is a complex and costly solution that may affect the functionality or performance of the applications, and it may not be feasible or practical in a 24/7 processing environment. Modifying the access management policy to make allowances for application accounts is a risky solution that may create exceptions or loopholes in the policy, and it may not comply with the best practices or standards for password management. Scheduling downtime to implement password changes is a disruptive solution that may affect the availability or continuity of the systems or applications, and it may not be acceptable or possible in a 24/7 processing environment. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.2.4

NEW QUESTION: 316
□□□□ □□□□ □□□□ □□□□□ □□□□□ □□□□□ □□□ □□□□□. □□ □ □□ □□□ □□□□□ □□□?
A. □□□ □□□□ □□□□ □□□□□ □□□□□.
B. □□□ □□□□□ □ □□□□□
C. □□□ □□□□□□
D. □□□ □□ □□□□ □□□□ □□□□□.
Answer: B (LEAVE A REPLY)
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: 317
IS □□□□ □□□ □□□□ □□□□□ □□□□ □□□ □□□□ □□□ □□□□□. □ □ □ □□□□ □ □□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□□ □□ □□□□.
B. □□□ □□ □□ □□□ □□□□□.
C. □□□ □□ □□□□□.
D. □□ □□□□□□ □□□□ □□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 318
□□□ □□□ □□□ □□□ □□ □□□□ □□□□ □□□ □□ □ □□□□ □□ □□ □□□ □□□□□. □□ □□□ □□ □ 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: 319
IS □□□□ □□ □□□ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□□□ □□ □□ □□□□. □□□□ □□ □ □□ □□ □□□ □□ □□□□ □□□□ □□□?
A. □□ □□□□□□ □□□ □□□□ □□□□.
B. □□ □□□□□ □□□□□ □□□□□.
C. □□□ □□□□ □□ □□□□ □□□□.
D. □□□ □□□ □□□□□□ □□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 320
□□ □□ □□□ □□ □□□ □□□ □□ □□□□□.
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: 321
□□□□ □□ □□□□ □□ □□□□ □□□□ □□ □□ □□ □□ □□□□ □□□□ □□ □□□ □□□□□?
A. □□□□ □□□
B. IS □□ □□□
C. □□□□□
D. □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 322
□□ □ □□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□ □□
C. □□□□ □□(CSA)
D. □□□□ □□□
Answer: C (LEAVE A REPLY)
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: 323
IS □□□□ IT □□ □□□□□ □□□□ □□ □□□ □□□□□□□□(PDCA) □□□ □□□□ □□□□ □ □□□ □□□ □□□□ □□□□□ □□□. □ □□□□ □□□□ PDCA □□□□□ □□ □□ □ □□ □□□ □□ □□□□ □□□?
A. □□
B. □□
C. □□□
D. □□
Answer: (SHOW ANSWER)
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: 324
□□ □ □□□□□ □□□ □□□□□□□ □□ □□□ □□ □□□ □□ □□ □□□□ □?
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: 325
□□ □ □□□ □□□ □□□□ □ □□□ □□ □□ □□□□ □□ □□ □□□□ □□□ □ □□ □□ □□□ □□□□□?
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: 326
□□□ □□□ □□ □□ □□, □□□□ □□□ □□□ □□□(ISP)□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□□□□ □□□ □□□□ □□. □□□ □□ □□□□□ □□□□□ □□□ □□□. □□□ □□ □□□ □□□□ □ □□.
A. □□□ □□□ □□□□ □□□□ □ □ □□□ □□□□ □□□□□□.
B. □□□ □□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □□□□□□□.
D. □□ □□□ □□□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The first step that the organization should take to ensure that only the corporate network is used for downloading business data is to include a statement in its security policy about Internet use. A security policy is a document that defines the rules, expectations, and overall approach that an organization uses to maintain the confidentiality, integrity, and availability of its data1. A security policy should clearly state the acceptable and unacceptable use of Internet resources, such as personalaccounts with ISPs, and the consequences of violating the policy. A security policy also helps to guide the implementation of technical controls, such as proxy servers, firewalls, or monitoring tools, that can enforce the policy and prevent or detect unauthorized Internet access.
The other options are not the first step that the organization should take, but rather subsequent or complementary steps that depend on the security policy. Using a proxy server to filter out Internet sites that should not be accessed is a technical control that can help implement the security policy, but it does not address the root cause of why users are

using personal accounts with ISPs. Keeping a manual log of Internet access is a monitoring technique that can help audit the compliance with the security policy, but it does not prevent or deter users from using personal accounts with ISPs. Monitoring remote access activities is another monitoring technique that can help detect unauthorized Internet access, but it does not specify what constitutes unauthorized access or how to respond to it.

References:

* ISACA CISA Review Manual 27th Edition (2019), page 247
* What is a Security Policy? Definition, Elements, and Examples - Varonis1

NEW QUESTION: 327

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

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: 328
□□ □□□□□ □□□ □□□□ □□ □ □□ □□□ □□ □□□□□?
A. □□ □□□□□ □□ □□ □□
B. □□ □□□□□ □□□ □□ □□
C. □□□ □□□□ □□□ □□□□□ □□ □□
D. □□□ □□ □□□□ □3□□ □□□ □
Answer: (SHOW ANSWER)

NEW QUESTION: 329
IS □□ □□(OA) □□□ □□□ □□□ □□□□□.
A. □□□□ □□ □□□ □□□ □□□ □□□□□ □□□□□.
B. □□□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
C. □□□ □□□□ □□□ □□□ □□□□□□ □□□□□.
D. □□□ □□ □□□ □□□ □□□□□□□.
Answer: (SHOW ANSWER)
The IS quality assurance (QA) group is responsible for ensuring that program changes adhere to established standards. Program changes are modifications made to software applications or systems to fix errors, improve performance, add functionality, or meet changing requirements. Program changes should follow established standards for documentation, authorization, testing, implementation, and review. The IS QA group is responsible for verifying that program changes comply with these standards and meet the expected quality criteria. Designing procedures to protect dataagainst accidental disclosure; ensuring that the output received from system processing is complete; and monitoring the execution of computer processing tasks are not responsibilities of the IS QA group. References: [ISACA CISA Review Manual 27th Edition], page 304.

NEW QUESTION: 330
□□□ □□ □□ □□ IS □□□□□ □□ □□□ □□□ □□ 3□ □□ □□ □□ □□□ □□□□ □□ □□□ □□□□□□□. □□ □ □□ □□□□ □ □□□ □□□□□?
A. □□ □□□ □□ □□ □□□ □□ □□ □□ □□□□ □□□□□.

B. □□ □□ □ □□□ □□□□ □□□□.
C. □□□ □□□ □□ □□□ □□ □□ □□□ □□□□□.
D. □□ □□□ □□ □□□ □□ □□ □□□ □□ □□□□□□.
Answer: D (LEAVE A REPLY)
The proximity badge incorrectly granting access to restricted areas is the most concerning issue, as it indicates a failure of the access control system to enforce the principle of least privilege and protect the sensitive or critical assets of the organization. The proximity badge should only grant access to the areas that are necessary for the IS auditor to perform the audit fieldwork, and not to any other areas that may contain confidential information, valuable equipment, or hazardous materials. The incorrect access could result in unauthorized disclosure, modification, or destruction of the assets, as well as potential safety or legal issues.
References
ISACA CISA Review Manual, 27th Edition, page 254
Office & Workplace Physical Security Assessment Checklist
Physical Security: Planning, Measures & Examples

NEW QUESTION: 331
IS □□□□ □□ □□□□ □□ □□ □□□□ □□ □□□□ □□□ □□□□ □□□□ □□□ □□□□□□.
IS □□□□ □□ □□□ □□ □ □□□□□ □□□?
A. □□ □□□ □□□ □□□□ □□□ □□□□□.
B. □ □□ □□□□□ □□□□ □□ □□□□□ □□□□□.
C. □ □□□ □□ □□□□ □□□ □□□□□.
D. □ □□□ □□ IT□□□ □□ □□□ □□□□.
Answer: B (LEAVE A REPLY)
The IS auditor's next course of action should be to report this control process weakness to senior management, as it may indicate a lack of oversight and accountability for the reporting system. Read-only users may have access to sensitive or confidential information that should be restricted or monitored. Periodic reviews of read-only users are a good practice to ensure that the access rights are still valid and appropriate for the users' roles and responsibilities. Reporting this weakness to senior management will also allow them to take corrective actions or implement compensating controls if needed.
Option A is incorrect because reviewing the list of end users and evaluating for authorization is not the IS auditor's responsibility, but rather the system owner's or administrator's. The IS auditor should only verify that such reviews are performed and documented by the responsible parties.
Option C is incorrect because verifying management's approval for this exemption is not sufficient to address the control process weakness. Even if there is a valid reason for not performing periodic reviews of read-only users, the IS auditor should still report this as a potential risk and recommend mitigating controls.

Option D is incorrect because obtaining a verbal confirmation from IT for this exemption is not adequate evidence or documentation. The IS auditor should obtain written approval from management and verify that it is aligned with the organization's policies and standards.
References:
CISA Review Manual (Digital Version)1, Chapter 1: The Process of Auditing Information Systems, Section
1.4: Audit Evidence, p. 31-32.
CISA Review Manual (Print Version), Chapter 1: The Process of Auditing Information Systems, Section 1.4:
Audit Evidence, p. 31-32.
CISA Online Review Course2, Module 1: The Process of Auditing Information Systems, Lesson 4: Audit Evidence, slide 9-10.
CISA Questions, Answers & Explanations Database3, Question ID: QAE_CISA_710.

NEW QUESTION: 332
□□□ □□□ □□ □□ □□□ □□ □□□ □□ □□ □□ □□ □□□ □□ □ □□□□ □?
A. □□ □□ □□□ □□□
B. □□□□□□ □□ □□□ □□□□ IT □□□ □□
C. □□□□ □□□□ □□
D. □□□ □□□ □□□□ □□ □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 333
□□ □□ □ □□ □□□ IT □□ □□ □□ □□□ □□□ □□□□ □□□?
A. □□□□
B. □□ □□ □□
C. □□□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
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: 334
□□□□□ □□□□ □□□□ □□□ □□□ □□□□□ □□□□ □□ □□□ □□□ □ □ □□ □ □□□ □□□□□□. □□ □□□ □□□ □□□□ □□□□?
A. □□
B. □□
C. □□
D. □□□
Answer: D (LEAVE A REPLY)
The type of control that is in place when an organization has established hiring policies and procedures designed specifically to ensure network administrators are well qualified is directive. Directive controls are those that guide or direct the actions of individuals or groups to achieve a desired outcome. Directive controls can also help to prevent or reduce the occurrence of undesirable events. Hiring policies and procedures are examples of directive controls that aim to ensure that only qualified and competent personnel are employed to perform IT-related tasks. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.11
* CISA Online Review Course, Domain 1, Module 2, Lesson 12

NEW QUESTION: 335
□□ □ P2P(□□□□□) □□□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□ □ □□□□□?
A. □□ □□ □□ □□ □□□□ □□□ □□□□□□.
B. □□ □□ □□□□□ □□□□ □□ □□□ □□□□□.
C. □□□ □□ □□ □□□(IDS)□ □□ □□□□□ □□□□□.
D. □□□□ □ □□□ □□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

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

NEW QUESTION: 337
IT □□□ □□□□ □□□ □□□□□ □□□ □, □□ □ □□ □□□ □□□ □□□□□?
A. □□□□□ □□
B. □□□ □□ □□□(ROI) □□ □□ ROI
C. □□ □□ □□ □□ □□
D. □□ □□ □□□(ROI) □□ □□ □□ ROI
Answer: B (LEAVE A REPLY)
The best way to determine whether IT investments are meeting business objectives is to compare therealized return on investment (ROI) versus the projected ROI(Option B). This approach measures actual performance against planned expectations.
ISACA CISA Reference:The ISACA IT Governance framework emphasizes performance measurement through ROI analysis, ensuring IT investments align with strategic objectives.
Risk Implication:If actual ROI is lower than projected, this may indicate ineffective investment decisions, poor execution, or misalignment with business goals.
Alternative Choices:
Option A:Break-even analysis only determines when an investment recoups its costs but does not measure performance against business objectives.
Option C:Budgeted versus actual spend assesses financial discipline but does not indicate business impact.
Option D:Industry average ROI provides benchmarking but does not assess internal goal achievement.

NEW QUESTION: 338
□□ □□□□□□ □□ □□ □□ □□□ □□□□ □□□ □□□□□□ □□ □□□ □□ □□□□□. □□ □ IS □□□□ □□ □□□ □□□□□ □□□?
A. □□□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□□.
B. □□□ □□□□ □□ □□□ □□□□□.
C. □□□□□□ □□□□□ □□□ □□□□□.
D. IT □□ □□□ □□□□□ □□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)
The IS auditor's next step after determining that many terminated users' accounts were not disabled is to perform a review of terminated users' account activity. This means that the IS auditor should check whether any of the terminated users' accounts were accessed or used after their termination date, which could indicate unauthorized or fraudulent activity. The IS auditor should also assess the impact and risk of such activity on the confidentiality, integrity, and availability of IT resources and data. The other options are not as appropriate as performing a review of terminated users' account activity, as they do not provide sufficient evidence or assurance of the extent and effect of the problem. References: CISA Review Manual, 27th Edition, page 240

NEW QUESTION: 339
□□ □ □□□□ □□□ □□(BCP)□ □□ □□ □□(DRP)□ □□ □□□□ □□□□ □ □□□□?
A. □□ □□□ □□ □□
B. □□□ □□□ □□
C. □□ □□□□ □□ □□
D. □□ □□□□ □□
Answer: C (LEAVE A REPLY)
The primary difference between a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) lies in their timeframe for activation and overall scope.
* BCP (Business Continuity Plan):
* Focuses on ensuring that critical business processes continue operating during and after a disruption.
* It includes strategies for maintaining operations (e.g., alternative work locations, manual procedures, supplier dependencies).
* Activated immediately when a disruption occurs to keep the business running.
* DRP (Disaster Recovery Plan):
* Primarily focuses on the recovery of IT systems and infrastructure after a disruption.
* It includes steps for restoring data, servers, and applications to bring IT operations back to normal.
* Activated after the disaster event to restore normal IT operations.
The timeframe for activation is the key difference because:
* BCP is implemented immediately to ensure business continuity.
* DRP is implemented after the disaster to restore IT operations.
* A. The annual testing requirements # Both BCP and DRP require regular testing, so this is not the key differentiator.
* B. The focus on system recovery # Only DRP focuses on system recovery, but the BCP covers more than just IT. The key difference is still the timeframe.
* D. The involvement of senior management # Senior management is involved in both plans, so this is not the primary distinction.

* ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience Why Not the Other Options?References:

NEW QUESTION: 340
IS □□□□ □□ □□□ □□□□□□ □□□ □□□ □□ □□□ □□□□ □□□□. □ □□ □□□ □□□□□ □□□□ □□ □□□ □□□□□□□. □□ □ □□ □□□□ □ □□□ □□□□□?
A. □□□ □□□ □□□
B. □□□ □□□ □□□
C. □□□ □□ □□□ □□□□□
D. □□□ □□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 341
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: 342
□□ □□□ □□□ □□□ □□□ □ IS □□□□ □□□□ □ □□ □□□ □□□ □□□ □□?

A. □□ □□ □□
B. □□□ □□ □□(SLA)
C. □□ □ □□ □□□□
D. □□□□ □□□
Answer: C (LEAVE A REPLY)
A maturity model for a technology organization is a tool that measures the progress and capability of the IT function in relation to its goals, processes, and practices. A maturity model can help identify gaps and areas for improvement, as well as benchmark the IT function against industry standards or best practices. One of the key aspects of a maturity model is the definition and clarity of roles and responsibilities for the IT function and its stakeholders. A roles and responsibility matrix, such as a RACI matrix, is a document that clarifies who is responsible, accountable, consulted, and informed for each task or deliverable in a project or process.
A roles and responsibility matrix can help avoid confusion, duplication, or omission of work, as well as ensure accountability and communication among the IT function and its customers, partners, and suppliers.
Therefore, an IS auditor should focus on reviewing the roles and responsibility matrix when evaluating the maturity model for a technology organization.
A standard operating procedure (SOP) is a document that describes the steps and instructions for performing a routine or repetitive task or process. SOPs are important for ensuring consistency, quality, and compliance in the IT function, but they are not directly related to the maturity model. A service level agreement (SLA) is a contract that defines the expectations and obligations between an IT service provider and its customers. SLAs are important for ensuring customer satisfaction, performance measurement, and dispute resolution in the IT function, but they are not directly related to the maturity model. A business resiliency plan is a document that outlines how an IT function will continue to operate or recover from a disruption or disaster. Business resiliency is important for ensuring availability, reliability, and security in the IT function, but it is not directly related to the maturity model. References: 1: Maturity Models for IT & Technology | Splunk 2: Responsibility assignment matrix - Wikipedia 3: Roles and Responsibilities Matrix - SDLCforms

NEW QUESTION: 343
□□ □□□□□ □□□ □□, □□□□ □□□□ □□□□ □□ □□ □□ □□□ □□ □ □□ □□ □ □□□□□?
A. □□ □□□ □□ □□□□
B. □□□□□ □□ □□□□
C. □□□ □□□□
D. □□□ □□□ □□□□ □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 344
□□□ □□ □□ □□ □□□□□ □□□□ □□□ □□□ □ IS □□□□ □□□□ □ □ □ □□□ □□□ □□□□□?
A. □□□□ □3□□ □□□ □□ □□□ □□□ □□□□ □□□□□.
B. □□□□ □□ □□ □□□ □□□□□.
C. □□□□ □□□ □□□□□ □□ □□□□ □□□ □□□□□.
D. □□□□ □□ □□ □□ □□□ □□ □□□ □□□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
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: 345

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

A. □□□ □□ □□.

B. □□ □□

C. □□ □□□ □□

D. □□ □□

Answer: A (LEAVE A REPLY)

When verifying the accuracy and completeness of migrated data for a new application system replacing a legacy system, it is most effective for an IS auditor to review data analytics findings. Data analytics is a technique that uses software tools and statistical methods to analyze large volumes of data and identify patterns, anomalies, errors or inconsistencies. Data analytics can help to compare the source and target data sets, validate the data quality and integrity, and detect any data loss or corruption during the migration process. The other options are not as effective, because audit trails only record the actions performed on the data, acceptance testing results only verify the functionality of the new system, and rollback plans only provide contingency measures in case of migration failure. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.6

NEW QUESTION: 346

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

A. □□□□ □□□

B. □□ □□(QA) □□□

C. □□□ □□

D. □□□□ □□□□ □□□

Answer: (SHOW ANSWER)

The business process owner is the most important stakeholder to involve in the review of the processes that prevent fraud within a business expense claim system. This is because the business process owner is responsible for defining, implementing, and monitoring the business rules and policies that govern the expense claim process. The business process owner also has the authority and accountability to approve or reject expense claims, as well as to investigate and report any suspicious or fraudulent activities. The business process owner can provide valuable insights and feedback to the IS auditor on the effectiveness and efficiency of the current processes, aswell as the potential risks and controls that need to be addressed12.

The information security manager is not the most important stakeholder because their role is mainly focused on ensuring the confidentiality, integrity, and availability of the information systems and data that support the expense claim process. The information security manager can help the IS auditor with assessing the technical aspects of the

system, such as access controls, encryption, logging, and backup, but they may not have sufficient knowledge or authority over the business rules and policies that prevent fraud1.
The quality assurance (QA) manager is not the most important stakeholder because their role is mainly focused on ensuring the quality and reliability of the software applications and systems that support the expense claim process. The QA manager can help the IS auditor with testing and verifying the functionality and performanceof the system, but they may not have sufficient knowledge or authority over the business rules and policies that prevent fraud1.
The business department executive is not the most important stakeholder because their role is mainly focused on overseeing the strategic objectives and financial performance of the business department that uses the expense claim system. The business department executive can help the IS auditor with understanding the business context and needs of the expense claim process, but they may not have sufficient knowledge or authority over the operational details and controls that prevent fraud

NEW QUESTION: 347
□□□□ □□□□ □□□□ □□ □□□□ □, □□□□□ □□□□ □□□□ □□ □□ □□□□ □□□□□ □ □□□□ □□□ □□ □□□□□.
A. □□□
B. □□□□ □□
C. □□
D. □□
Answer: (SHOW ANSWER)
Compared to developing a system in-house, acquiring a software package means that the need for testing by end users is unchanged. This is because end users are still the ultimate customers and beneficiaries of the system, and they need to ensure that the software package meets their requirements, expectations, and satisfaction. End user testing, also known as user acceptance testing (UAT) or beta testing, is the final stage of testing performed by the user or client to determine whether the software can be accepted or not1.
End user testing is important for both in-house developed and acquired software packages, as it helps to verify the functionality, usability, performance, and reliability of the system2. End user testing also helps to identify and resolve any defects, errors, or issues that may not have been detected by the developers or vendors3.

Therefore, option B is the correct answer.
Option A is not correct because end user testing is not eliminated by acquiring a software package. Even though the software package may have been tested by the vendor or supplier, it may still have bugs, compatibility issues, or configuration problems that need to be fixed before deployment4. Option C is not correct because end user testing is not increased by acquiring a software package. The scope and extent of end user testing depend on various factors, such as the complexity, criticality, and customization of the system, and not on whether it is developed in-house or acquired. Option D is not correct because end user testing is not reduced by acquiring a software package. The software package may still require modifications or integrations to suit the specific needs and environment of the organization, and these changes need to be tested by the end users.
References:
Chapter 4 Methods of Software Acquisition5
What is User Acceptance Testing (UAT): A Complete Guide1
What Is End-to-End Testing? (With How-To and Example)3
How to Evaluate New Software in 5 Steps4
User Acceptance Testing (UAT) in ERP Projects
User Acceptance Testing for Packaged Software

NEW QUESTION: 348
□□□ □□□ □□ □□□ □□□□ IS □□□□ □□□ □□ □□ □□ □□□ □□□□.
A. □□□ □□ □ □□□ □□□ □□□□ □□□□.
B. □□□ □□ □□□ □□ □□□□ □□□ □□□□.
C. □ □□□ □□ □□□□ □□ □□□□□□□.
D. □□ □□□ □□□ □□□□□□□.
Answer: B (LEAVE A REPLY)
An IS auditor reviewing the threat assessment for a data center would be most concerned if all identified threats relate to external entities. This indicates that the threat assessment is incomplete and biased, as it ignores the potential threats from internal sources, such as employees, contractors, vendors, or authorized visitors. Internal threats can pose significant risks to the data center, as they may have access to sensitive information, systems, or facilities, and may exploit their privileges for malicious or fraudulent purposes. According to a study by IBM, 60% of cyberattacks in 2015 were carried out by insiders1
Some of the identified threats are unlikely to occur is not a cause for concern, as it shows that the threat assessment is comprehensive and realistic, and considers all possible scenarios, regardless of their probability.
A threat assessment should not exclude any potential threats based on subjective judgments or assumptions, as they may still have a high impact if they materialize.
The exercise was completed by local management is not a cause for concern, as it shows that the threat assessment is conducted by the people who are most familiar with the data center's operations, environment, and risks. Local management may have more relevant

and accurate information and insights than external parties, and may be more invested in the outcome of the threat assessment.
Neighboring organizations' operations have been included is not a cause for concern, as it shows that the threat assessment is holistic and contextual, and considers the interdependencies and influences of external factors on the data center's security.
Neighboring organizations' operations may pose direct or indirect threats to the data center, such as physical damage, network interference, or shared vulnerabilities.
References:
* IBM Security Services 2016 Cyber Security Intelligence Index 1

NEW QUESTION: 349
□□□ □□ □□□ □□□□□□□ □□□□ □□□ □□□ □□□□□□ □□□ □□□ □□□ □□□ □□□□□. □□ □ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□ □□□?
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: 350
□ □□□ □□ □□□□ □□□ □□□□ □□ □□□ □□□□ □□□□□□ □□□□ □ □□□□□. □□ □ □□ □□ IS □□□□ □□□□ □□ □□ □□□ □□□ □□ □ □□ □□□□?
A. □□ □□□□ □□□□ □□ □□□ □ □□ □□□ □□□□□.
B. □□□ □□□ □□□□ □□□□ □□ □□ □ □□ □□ □□□□ □□□□□.
C. □□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.
D. □□□□ □□□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 351
□□□ □□□□□□ □□ □□ □□□□ □□□□ □□□□□ □□ □□□□. □□ □□□ □ □□ □□(BIA)□ □□ □□□□ □□□?
A. □□□ □□ □□□ □□□□ □□
B. □□□ □□ □□□ □□□□ □□
C. □□ □ □□ 1□
D. □□ □□□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 352
IS □□□□ □□□□ □□□ □□ □□□□ □□□□□□ □□□□□ □□□□□(API)□ □□□□ □□ □□□□□□□ □□ □□□ □□□ □□□□□ □□ □□□□□□. □ □□ □ □□□□ □□ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□□ □□ □□ □□□□□□ □□□□ API □ □□ □□□ □□□□□.
B. □□ □□□□□□□□ □□ □□ □□□□ □□□□□ API □□ □□□□□.
C. API □□ □□□□ □□ □□□ □□□ □□□□ □□ □□ □□□□ □□□□□.
D. □□□ □□□ □□□ □□ □ API □□ □□□□□ □□□□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 353
□□ □□ □□□□ □□□□□ □□□□□□□. □□ □□ □□□□ □□ □□□□ □□□ □□□□□.
A. □□□ □□ □□ □□(UPS) □□□ □□ □□□ □□□□
B. □□ □□□□ □□ □□□ □□□□
C. □□□ □□□ □□□
D. □□ □□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
A fire alarm system is a device that detects and alerts people of the presence of fire or smoke in a building. A fire alarm control panel is the central unit that monitors and controls the fire alarm system. The most effective location for the fire alarm control panel would be inside the booth used by the building security personnel.
This is because:

* The security personnel can quickly and easily access the fire alarm control panel in case of an emergency, and take appropriate actions such as notifying the fire department, evacuating the building, or resetting the system.
* The fire alarm control panel can be protected from unauthorized access, tampering, or damage by the security personnel, who can also monitor its status and performance regularly.
* The fire alarm control panel can be isolated from the computer room, which may be exposed to higher risks of fire or smoke due to the presence of electrical equipment, such as uninterruptible power supply (UPS) modules or server computers.
* The fire alarm control panel can be connected to the computer room through a dedicated communication line, which can ensure reliable and timely transmission of signals and information between the two locations.
References:
* [1]: Fire Alarm Control Panel - an overview | ScienceDirect Topics
* [2]: Fire Alarm Control Panel - What is it and how does it work? | Fire Protection Online
* [3]: Fire Alarm Control Panel Installation Guide - XLS3000 - Honeywell

NEW QUESTION: 354
IS □□□□ □□□□ □□□□□ □□□□□□ □□□□ □□□□ □□ □□□□□□. □ □ □ □□□□ □□ □□□ □□□□□?
A. □□ □□□ □□□□□.
B. □□□ □□ □□□ □□□□□.
C. □□□□ □□ □□□□□.
D. □□□□ □□□□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The IS auditor's next course of action after finding that firewalls are outdated and not supported by vendors should be to determine the risk of not replacing the firewall. Outdated firewalls may have known vulnerabilities that can be exploited by attackers to bypass security controls and access the network. They may also lack compatibility with newer technologies or standards that are required for optimal network performance and protection. Not replacing the firewall could expose the organization to various threats, such as data breaches, denial-of-service attacks, malware infections, or regulatory non-compliance. The IS auditor should assess the likelihood and impact of these threats and quantify the risk level for management to make informed decisions.

NEW QUESTION: 355
□□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□□□□ □□□ □□□ □□□□□.
B. □□□□ □□□ □□□□□.
C. □□ □□□ □□□□□.
D. □□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)
The best way to address segregation of duties issues in an organization with budget constraints is to implement compensating controls, which are alternative controls that reduce or eliminate the risk of errors or fraud due to inadequate segregation of duties. Compensating controls may include independent reviews, reconciliations, approvals, or supervisions. Rotating job duties periodically may reduce the risk of collusion or abuse of privileges, but it may also affect operational efficiency and continuity. Performing an independent audit may detect segregation of duties issues, but it does not prevent them. Hiring temporary staff may increase operational costs and introduce new risks.
References: CISA Review Manual (Digital Version), Chapter 2, Section 2.4

NEW QUESTION: 356
□□ □ □□ □□ □□□ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□□ □□□□□□.
B. □□□□ □□□□ □□□□□ □□□□□□ □□□ □□□□□.
C. □□ □□□ □□□□ □□ □□□□ □□□□□.
D. □□ □□□□□ □□□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
Operational log management primarily enhances security by enabling real-time monitoring and detection of anomalies within network data. Logs provide valuable information for identifying threats, investigating incidents, and ensuring compliance with security policies.
* Predictive Analysis for User Experience (Option A):While logs may support analytics, this is not the primary benefit.
* Performance Issue Identification (Option C):Logs can help identify performance issues, but the focus of operational log management is security.
* Data Aggregation Using Unified Storage (Option D):This supports management but is secondary to the security benefits.
Reference:ISACA CISA Review Manual, Job Practice Area 3: Information Systems Operations and Business Resilience.

NEW QUESTION: 357
□□ □□□ Agile □□□□ □□ □□□□ □□□□ □□□ ERP(Enterprise Resource Planning) □□□□ □□□□ □□ □□ □□□□ □□□□ □□□□. □ □□□□ □□□ □ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□
B. Agile □□□□ □□ □□
C. □□□ □□ □□□ □□□ □ □□ □□
D. ERP □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 358

□□ □ □□ □□ □□□□□ □□□ □□□ □□□□ □□ □□□□ □□ □□□□□?
A. □□ □□□ □□ □□□ □□□□ □□ □□□ □□□□□ □□□□□□ □□□□□.
B. □□ □□□□ □□□ □□ □□□ □□□ □□□□ □□□ □□ □□□ □□□□□.
C. □ □□□ □□ □□□ □□□□ □□□ □□□ □□□□□ □□
D. □□ □□ □ □□□ □□□□ □□□ □□ □□ □□ □□ □□
Answer: B (LEAVE A REPLY)
Data analytics can be used to compare data from different sources and identify any discrepancies or anomalies. In this case, comparing a population of loans input in the origination system to loans booked on the servicing system can help detect any errors or frauds in the loan origination process. The other options are not examples of data analytics, but rather controls for data integrity, reconciliation, and error handling. References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3.2

NEW QUESTION: 359
□□ □ □□ □□□ □□ □□ □ □□□ □□□ □□□□ □□□□ □ □□□ □□ □□□ □□□□ □ □□ □□□□□?
A. □□ □□□ □□ □□ □□□ □□□□□
B. □□ □□□□ □□ □□ □□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□ □□□□□ □□□□□□.
D. □□□□ □□□ □□ □□□□ □□ □□□□□
Answer: (SHOW ANSWER)
The best way to ensure that a backup copy is available for restoration of mission critical data after a disaster is to periodically test backups stored in a remote location. Testing backups is essential to verify that the backup copies are valid, complete, and recoverable. Testing backups also helps to identify any issues or errors that may affect the backup process or the restoration of data. Storing backups in a remote location is important to protect the backup copies from physical damage, theft, or unauthorized access that may occur at the primary site. Using an electronic vault for incremental backups, deploying a fully automated backup maintenance system, or using both tape and disk backup systems are not sufficient to ensure that a backup copy is available for restoration of mission critical data after a disaster, as they do not address the need for testing backups or storing them in a remote location. References: Backup and Recovery of Data: The Essential Guide | Veritas, The Truth About Data Backup for Mission-Critical Environments - DATAVERSITY.

NEW QUESTION: 360
□□□ □□ □□ □□(DRP)□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □ □□□□?
A. DRP□ IT □□□□ □□□□□□□.
B. DRP□ □□ 3□ □□ □□□□□ □□□□□.
C. DRP□ 2□ □□ □□□□□□ □□□□□.
D. DRP□□ □□ □□□□ □□ □□ □□(RTO)□ □□□□ □□□□.

Answer: B (LEAVE A REPLY)
The DRP is a set of procedures and resources that enable an organization to restore its critical IT functions and operations in the event of a disaster or disruption. The DRP should be tested regularly to ensure its effectiveness, validity, and readiness. Testing the DRP can help to identify and resolve any gaps, issues, or weaknesses in the plan, as well as to evaluate the performance and capability of the recovery team and resources. If the DRP has not been tested during the past three years, it may not reflect the current IT environment, business requirements, or recovery objectives, and it may fail to meet the expectations and needs of the stakeholders.
References
ISACA CISA Review Manual, 27th Edition, page 255
Disaster Recovery Plan Testing: The Ultimate Checklist
What is a Disaster Recovery Plan (DRP) and How Do You Write One?

NEW QUESTION: 361
□□ □□□ □□□□ □□□□□□ □□□□ □□□ □□□□ □ □□ □□ □ □□□ □ □ □ □□□□□?
A. □□ □□□ □□□□□□ □□□□□.
B. □□ □□ □□□ □□□ □□ □□□□□ □□□□□□□.
C. □□□ □□□□ □□□□ □□□ □ □□□□.
D. □□□ □□ □□ □□□ □□□ □□□ □ □□□□.
Answer: D (LEAVE A REPLY)
The greatest risk associated with security patches being automatically downloaded and applied to production servers is that patches may result in major service failures, as they may introduce new bugs, conflicts, or incompatibilities that could affect the functionality, performance, or availability of the servers12. Automatic patching may also bypass the testing and validationprocesses that are necessary to ensure the quality and reliability of the patches34.
References
1: Do you leave Windows Automatic Updates enabled on your production IIS server? - Server Fault1 2:
Azure now installs security updates on Windows VMs automatically3 3: Server Patch Management | Process of Server Patching - ManageEngine2 4: Windows Security Updates | Microsoft Patch Updates Guide - ManageEngine4

NEW QUESTION: 362
□□□□□ □□□ □□ □□□ □□□ □□□ □□□□ □□ □□□□□ □□ □□ □□ □□ □□□ □□ □ □□ □□□?
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: 363
□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□, □□□ □□□□□□ □□□□ □ □ 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: 364
□□ □□□□ □□□□□□□ □□□ □□ □ □□□ □□□□□?
A. □□□ □□
B. □□□ □□
C. □□ □□ □□
D. □□□ □□□□□
Answer: (SHOW ANSWER)
A single point of failure is a component or system that, if it fails, will cause the entire system to stop functioning. In virtual environments, the hypervisor is the software layer that enables multiple virtual machines to run on a single physical host. If the hypervisor is compromised, corrupted, or unavailable, all the virtual machines running on that host will be affected. This can result in data loss, downtime, or security breaches.
References
ISACA CISA Review Manual, 27th Edition, page 254
Virtualization: What are the security risks?
What Is a Hypervisor? (Definition, Types, Risks)

NEW QUESTION: 365

IT □□□□ □□□ IT □□□ □□□ □□□□□ □□□□ □□□□□ □□□□□ □□□ □□□□□ □□□. □□ □ □□ □□ □□ □□□ □□□□□?
A. □□ □□ □□(KPI)□ □□□□□.
B. □□ □□ □□(CSA)□ □□□□□.
C. □□□ □□□ □□□□□.
D. □ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 366
□□ □ □□ □□ □□□□ □□□□ □□ □□□ □□□□ □□ □□□□□?
A. □□□ □□ □□ □□ □□□ □□□□□.
B. □□□ □□□□□ 3□ □□□□ □□□ ID□ □□□□□.
C. □□□□ □□ □□ □□□□ □□ □□ □□□□ □□□□ □□□.
D. □□ □□□□ □□ □□ □□ □□(DRP)□ □□□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 367
□□ □ □□□□ □□□ □□(BCP)□ □□□ □□□□ □□ □□ □□□□ □□□ □□□ □□?
A. □□□□ □□
B. □□□□ □□□
C. □□ □□ □□□
D. □□ □ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 368
□□□ □□ □□□ □□□□ □□□□ □□□□□?
A. IT □□ □□□
B. □□□ □□□
C. □□□□□□ □□□(DBA)
D. □□□□ □□□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Thedata owneris the individual or entity responsible for classifying, protecting, and defining access permissions to data. They ensure that only authorized personnel can access, modify, or distribute data based on business needs and regulatory requirements.
* Data Owner (Correct Answer - B)
* The data owner is responsible forsetting user permissionsbased on job roles and business requirements.
* According toISACA's CISA Review Manual and COBIT 2019, the data owner determines access levels while IT personnel enforce them.

* Example:A finance department head (data owner) determines that only certain accountants should access sensitive payroll data.
* IT Operations Manager (Incorrect - A)
* Oversees IT infrastructure but does not define data access controls.
* Database Administrator (DBA) (Incorrect - C)
* Implements and enforces security settings but follows rules set by the data owner.
* Information Security Manager (Incorrect - D)
* Provides security guidance but does not decide specific access permissions.
References:
* ISACA CISA Review Manual
* COBIT 2019 Framework
* NIST 800-53 (Security and Privacy Controls for Federal Information Systems)

NEW QUESTION: 369
IS □□□□ IS □□□ □□ □□□ □□□□□ □□□□□□□. IS □□□□□ □□□ □ □, □□□□ □□□□□ □□□ □□ □□□ □□□ □□ □□ □□□□□. □□ □ □□□ □ □□ □□□ □□□□□?1
A. IS □□□ □□□ □□ □□□ □□ □□ □□□ □□□□□.
B. IS □□□□ □□ □□□ □□□ □□□ □□□ □□□□□.
C. □□□ □□ □□□ □□ □□□ □ □□
D. □□□ □□□□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
The auditor's next action after finding that there is an informal unwritten set of standards in the IS department is to document and test compliance with the informal standards. This is because the auditor's role is to evaluate the adequacy and effectiveness of the existing controls, regardless of whether they are formal or informal, written or unwritten. The auditor should also assess the risks and implications of having informal standards, such as lack of consistency, accountability, or traceability. The auditor should not make recommendations, postpone the audit, or finalize the audit without performing the audit procedures.
References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.21
* CISA Online Review Course, Domain 1, Module 1, Lesson 12

NEW QUESTION: 370
IS □□□□ □□□□□ □□□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□□. □ □□□ □□□□ □□ □□□□ □□ □ □□ □□ □□□ □□□□□ □□□□ □□□?
A. □□ □□ □ □□□ □□ □□
B. □□□ □□ □□(SLA)
C. □□□□□ □□□□ □□
D. □□□ □□

Answer: C (LEAVE A REPLY)
The correct answer is C. Software escrow agreement. A software escrow agreement is a legal arrangement between three parties: the software developer (licensor), the end-user (licensee), and an escrow agent. The agreement ensures that the software's source code and other relevant assets are securely stored with the escrow agent, and can be released to the licensee under certain conditions, such as the licensor's bankruptcy, insolvency, or failure to provide support or maintenance1. A software escrow agreement can provide the licensee with assurance and continuity for the software they depend on, and protect them from losing access or functionality in case of any unforeseen events or disputes with the licensor1.

NEW QUESTION: 371
□□ □ □□ □□□ □□□□ □□□□ □□□□ □□□□□□□□ □□□□ □□□□ □ □□ □□□□□?
A. □□□
B. □□
C. □□□□
D. □□
Answer: C (LEAVE A REPLY)
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: 372
□□ □□ IS □□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□ □□ □□ □□ □□□ □□□ □□□□ □□
B. □□□ □□ □□, □□ □ □□□ □□□□□.
C. □□ □□ □□□ □□□□ □ □□□ □□□ □□□ □□□□
D. □□ □□□ □□□□ □□ □□□□□ □□□ □ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 373
□□ □□ □□(DRP) □□□□ □□□□□□□ □□□□ □□ □□ □□□ □□ □ □□□ □□?
A. □□ □□□ □□□ □□□ □□□□□□ □□□□□.
B. □□ □□□ □□□□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□□□.
D. □□□□□ □□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)
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: 374
□□ □ □□ □□□□ □□□ □□□□□ □□□□ □□ □ □□□ □□□□□?
A. □□ □□□□□ □□□□□ □□□□□ □ □□□□.
B. □□ □□□ □□□ □□ □□□ □□□ □ □□□□.
C. □□□ □□□ □□□ □□□ □□□□□□ □□□□□□□□ □ □□□□.
D. TCP/IP(□□ □□ □□□□/□□□ □□□□)□ □□ □ □□ □□□ □□ □□□ □□□ □□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 375
□□□ □□ □□□□□ □□□□□ □□□□ 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: 376
□□□□□ □□ □□ □ □□□ □□□□ □□□□ □□□.
A. □□ □□□.
B. □□□□□□ □□□(DBA).
C. □□□□ □□□.
D. □□□.
Answer: (SHOW ANSWER)
The business owner is the person or entity that has the authority and responsibility for defining the purpose and scope of the processing of personal data, as well as the expected outcomes and benefits. The business owner is also accountable for ensuring that the processing of personal data complies with the applicable laws and regulations, such as the General Data Protection Regulation (GDPR) or the Data Protection Act 2018 (DPA 2018). One of the requirements of the GDPR and the DPA 2018 is to adhere to the principle of storage limitation, which states that personal data should be kept for no longer than is necessary for the purposes for which it is processed1. This means that the business owner should determine and justify how long they need to retain personal data, based on factors such as:
The nature and sensitivity of the personal data
The legal or contractual obligations or rights that apply to the personal data The business or operational needs and expectations that depend on the personal data The risks and impacts that may arise from retaining or deleting the personal data The business owner should also establish and document the conditions and methods for the destruction of personal data, such as:
The criteria and triggers for deciding when to destroy personal data
The procedures and tools for securely erasing or anonymising personal data The roles and responsibilities for carrying out and overseeing the destruction of personal data The records and reports for verifying and evidencing the destruction of personal data
Therefore, retention periods and conditions for the destruction of personal data should be determined by the business owner, as they are in charge of defining and managing the processing of personal data, as well as ensuring its compliance with the law.

NEW QUESTION: 377
□□ □□ □□□ □ □□ □□□ □□□ □□□□.
A. □□□ □□□□□.
B. IT □□□□□ □□□□.
C. □□□ □□ □□□ □□ □□□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The first step in an incident response plan is typically preparation12. However, among the options provided, validating the incident would be the first step. This involves confirming that a security event is actually an incident3. It's important to verify the event to avoid wasting resources on false positives.
References:
Incident Response Plan: Frameworks and Steps - CrowdStrike
What is Incident Response? Plan and Steps | Microsoft Security
What Are the Phases of an Incident Response Plan? - ISC2 Blog

NEW QUESTION: 378
□□ □ □□□□□□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□□□□?
A. □□□□□ □□ □□□ □□□ □□□□□.
B. □□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□□□.
C. □□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□□.
D. □□ □□(QA) □□ □□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
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: 379
□□ □□□ □□ □□□ □□□ □□□ □ □□□□.

A. □□ □□ □□
B. □□□□ □□ □□□ □□□ □□□□□.
C. □□□□□ □□ □□ □□□□□□□ □□□ □□□□□.
D. □□□□ □□□□ □□□□□.
Answer: C (LEAVE A REPLY)
Capacity management is a process that ensures that the IT resources of an organization are sufficient to meet the current and future demands of the business. Capacity management enables organizations to identify the extent to which components need to be upgraded, by monitoring and analyzing the performance, utilization, and availability of the IT components, such as servers, networks, storage, applications, etc., and identifying any bottlenecks, gaps, or risks that may affect the service level agreements (SLAs) or quality of service (QoS). Capacity management also helps organizations to plan and optimize the use of IT resources, by forecasting the future demand and growth of the business, and aligning the IT capacity with the business needs and objectives. Forecasting technology trends is a possible outcome of capacity management, but it is not its main purpose. Establishing the capacity of network communication links is a part of capacity management, but it is not its main goal. Determining business transaction volumes is an input for capacity management, but it is not its main objective.

NEW QUESTION: 380
IT □□□□ □□ □□ IS □□□□ IT □□□ □□□ □□□□□ □□□□ □□□□□□ □ □□□ □□ □□□□□. IS □□□□□ □□ □ □□□ □□□ □□□ □□□ □□ □□ □ □□□ □□□□.
A. □□ □□□ □□□□□.
B. □□□ □□□□ □□ □□□□ □□ □□□ □□□□□.
C. □□ □□□ □□ □□□ □□□□□.
D. □□□ □□ □□(QA)□ □□□ □□□.
Answer: A (LEAVE A REPLY)
The greatest concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated is that policies and procedures might not reflect current practices. Policies are documents that define the goals, objectives, and guidelines for an organization's information systems and resources. Procedures are documents that describe the steps, tasks, or activities for implementing or executing policies. Policies and procedures should be regularly reviewed and updated to ensure that they are relevant, accurate, consistent, and effective for the organization's information systems and resources. Policies and procedures that are not regularly reviewed and updated might not reflect current practices, as they might be outdated, obsolete, or incompatible with the current state or needs of the organization's information systems and resources. This can cause confusion, inconsistency, inefficiency, or noncompliance among users or stakeholders who rely on policies and procedures for guidance or direction. Policies and procedures might not include new systems and corresponding process changes is a

possible concern for an IS auditor when reviewing IT policies and procedures that are not regularly reviewed and updated, but it is not the greatest one. Policies and procedures might not include new systems and corresponding process changes, as they might be unaware of or unresponsive to the introduction or modification of information systems or resources within the organization. This can cause gaps, overlaps, or conflicts among policies and procedures that affect different information systems or resources.

NEW QUESTION: 381
IS □□□□ □□□ □□□ □□□□□□□ □□□ □□□□ □□□□ □□□□ □□□ □ □□ □□ □□ □□□□ □□ □ □□□ □□ □□□□□□. □□ □ □□ □□ □□□□ □ □□□ □□□□□□□□ □□ □□ □ □□□□□□?
A. □□ □□(QA) □□□□ □□□ □□□ □□ □□□
B. □□□ □□□□□□ □□ □□ □□ □□□□ □□
C. □□□□ □□□□ □□ □□□□ □□□□ □□ □□□ □□ □□ □□(SDLC) □ □□ □□
D. □□□□□□ □□□ □□ □□□□□□ □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 382
□□ □ □3□ □□□ □□□□□ □□ □□ □□□ □□□□□□ □□ □□□□ □□ □□ □□□ □□□□□?
A. □□□ □□□□ □□ □□□□ □□ □□□ □□ □□ □□□
B. □□□ □□□□ □□ □□ □□□ □□ □□
C. □□□ □□□□ □□□□□□□□□ □□□
D. □□□ □□□□ □□ □ □□ □□
Answer: A (LEAVE A REPLY)
An audit report of the controls by the service provider's external auditor provides the best evidence that a third-party service provider's information security controls are effective. An external auditor is an independent and objective party that can assess the design and operating effectiveness of the service provider' s information security controls based on established standards and criteria. An external auditor can also provide an opinion on the adequacy and compliance of the service provider's information security controls, as well as recommendations for improvement.
Documentation of the service provider's security configuration controls is a source of evidence that a third- party service provider's information security controls are effective, but it is not the best evidence.
Documentation of the security configuration controls can show the settings and parameters of the service provider's information systems and networks, but it may not reflect the actual implementation and operation of the controls. Documentation of the security configuration controls may also be outdated, incomplete, or in accurate.

An interview with the service provider's information security officer is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. An interview with the information security officer can provide insights into the service provider's information security strategy, policies, and procedures, but it may not verify the actual performance and compliance of the information security controls. An interview with the information security officer may also be biased, subjective, or misleading.
A review of the service provider's policies and procedures is a source of evidence that a third-party service provider's information security controls are effective, but it is not the best evidence. A review of the policies and procedures can show the service provider's information security objectives, requirements, and guidelines, but it may not demonstrate the actual execution and enforcement of the information security controls. A review of the policies and procedures may also be insufficient, inconsistent, or outdated.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 284
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription

NEW QUESTION: 383
□□□□□ □□ □□□□ □□□ □□□ □, e-□□ □□□ □□□ □□□□□□ □□ □ □□□ □□□□□?
A. □□ □□ □□
B. □□□ □□□□ □□ □□
C. □□□ □□ □□□□ □□
D. □□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
Outsourcing the development of an e-banking solution when in-house technical expertise is not available can significantly reduce start-up costs. This is because the organization can avoid the expenses associated with hiring and training a full-time development team, purchasing necessary hardware and software, and maintaining the system1. While outsourcing can also potentially reduce the risk of system downtime, increase the ability to adapt the system, and provide direct oversight of risks, these benefits are not as immediate or guaranteed as the cost savings123.
References: Maxicus1, Forbes2, Strategy& - PwC3

NEW QUESTION: 384
□□ □□□□□ □□ □□□ □□□ □, □□ □ □□ □□ □□ □ □□ □□□□□?
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: 385
□□ □ □□□□ IT □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. IT □□□ □□□ □□ □□ □□(SDLC)□ □□ □□□□ □□□□□□□.
B. IT □□□ □□ □□□□ □□□ □□□□□.
C. IT □□□ □□□ □ □□□ □□ □□ □□ □□(KPI)□ □□□□□.
D. IT □□ □□□ □□ □□□□□□ □□□ □□□□.
Answer: B (LEAVE A REPLY)
This means that the IT investments are aligned with the strategic goals and priorities of the organization, and that they deliver value and benefits to the business. Mapping IT investments to specific business objectives can help ensure that the IT investments are relevant, justified, and measurable, and that they support the organization's mission and vision.
IT investments are implemented and monitored following a system development life cycle (SDLC) is an indication of effective IT project management, but not necessarily of effective IT investment management.
The SDLC is a framework that guides the development and implementation of IT systemsand applications, but it does not address the alignment, justification, or measurement of the IT investments.
Key performance indicators (KPIs) are defined for each business requiring IT investment is an indication of effective IT performance management, but not necessarily of effective IT investment management. KPIs are metrics that measure the outcomes and results of IT activities and processes, but they do not address the alignment, justification, or value of the IT investments.

The IT investment budget is significantly below industry benchmarks is not an indication of effective IT investment management, but rather of low IT spending. The IT investment budget should be based on the organization's needs and capabilities, and not on external comparisons. A low IT investment budget may indicate that the organization is underinvesting in IT, which could limit its potential for growth and innovation.

NEW QUESTION: 386
□□ □□□□□□ □□□ □□ □□□□ IS □□ □□□ □□□ □ □□□□.
A. □□□ □□□□ □ □□□ □□□□ □□□ □□□□□.
B. □□ □□□□□ □□□□ □□□ □□ □□□□ □□.
C. IS □□ □□□ □□□ □□□ □□□□□.
D. □□ □□□ □□□ □□ □ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 387
IS □□□□ □□□□□ □□□□□ □□□□□, □□ □□ □□□□ □□ □□□□□ □□ □□□□.
□□ □□□ □□□□ □□ □□ IS □□□□ □□□ □ □□ □□ □□□ □□ □ □□□□ □?
A. □□ □□□□□□□ □□□ □□□ □□ □□□ □□□□.
B. □□□□□ □□□□□□□ □□□ □□□ □□ □□□ □□□□.
C. □□ □ □□ □□□ □□□□□□□ □□□□ □□□□ □□ □□□ □□□□.
D. □□ □□ □□□ □□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 388
□□□ □□□□ □□□□ □□□ □□ □□□ □□□ □□ IS □□□□ □□ □□□□ □ □□□ □□□□□?
A. □□□□ □□□□ □□□□ □□ □□□ □□□□ □□ □ □□□□.
B. □□□ □□□□ □□□□ □□□□□ □□□ □ □□□□.
C. □□□□ □□□□ □ □ □□□□.
D. □□ □□□ IT □□□ □□□ □□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)
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: 389
□□□□□□ □□ □□ □ □□ □□ □□□□ □□□ □□□ □□ □ □□ □ □□ □□ □ □□□ □□ □□ □□□□□?
A. □□□ □□□ □□□□.
B. □□□□ □□□□□.
C. □□□ □□ □□
D. □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The rules of engagement define the scope, objectives, methodology, deliverables, and limitations of the penetration testing. They also specify the legal and ethical boundaries, communication channels, and escalation procedures. Establishing the rules of engagement is the first step when planning to conduct penetration testing for a client, as it

ensures that both parties agree on the expectations and outcomes of the testing. The other options are important steps, but they should be done after the rules of engagement are established. References: CISA Review Manual (Digital Version) 1, page 381.

NEW QUESTION: 390
□□ □ □□□□□□ □□□□(EA) □□□□□ □□ □□□ □□□□□?
A. □□□ □□□□□ □□□ □□ □□□□□ □□□ □□□□ □□□□□.
B. EA□ □□□ □□ □□□ □□□ □ □□□ □□□□□.
C. EA□ □□ □□ □ □□□ □□□□□ □□□□□.
D. □□□ □□□□□□ □□ □□□ □□ □□□(ROI)□ □ □ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
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: 391
□□□ □□□□ □□ □□□□□ □□□□ □ □□□ □□ □□ □□□ □□□ □□□ □ □ □ □□ □□□□?
A. □□□ □□□ □□ □□ □□
B. □□ □□□□ □□□□ □□ □□□ □□
C. □□ □□□ □□□□ □□□ □□□ □□ □□
D. □□ □□□ □□□ □□□□□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
Analyzing risks posed by new regulations is an appropriate role of internal audit in helping to establish an organization's privacy program. An internal auditor can provide assurance and advisory services on the compliance and effectiveness of the privacy program, as well

as identify and assess the potential risks and impacts of new or changing privacy regulations. The other options are not appropriate roles of internal audit, but rather the responsibilities of the management, the information security officer, or the privacy officer.
References:
* CISA Review Manual (Digital Version), Chapter 7, Section 7.4.21
* CISA Review Questions, Answers & ExplanationsDatabase, Question ID 216

NEW QUESTION: 392
□□ □□□ □□□□ □□ BEST□ IT□ □□□□ IT □□ □□□□ □□□ □□□□□.
A. □□□ □□□□ □□ □□□ □□□ □□□□.
B. □□□□□ □□ □□ □□□□□.
C. □□□□□□ □□□□(EA)□ □□.
D. □□□ □□□ □□□ IT □□.
Answer: C (LEAVE A REPLY)
An IT strategic plan that best leverages IT in achieving organizational goals will include enterprise architecture (EA) impacts. EA is the practice of analyzing, designing, planning, and implementing enterprise analysis to successfully execute on business strategies1. EA helps organizations structure IT projects and policies to align with business goals, to stay agile and resilient in the face of rapid change, and to stay on top of industry trends and disruptions1. EA also describes an organization's processes, information processes and personnel and other organizational subunits aligned with the organization's core goals and strategies2. By including EA impacts in the IT strategic plan, an organization can ensure that the IT initiatives are consistent with the business vision, objectives, and tactics, and that they support the desired business outcomes3.
A comparison of future needs against current capabilities, a risk-based ranking of projects, and IT budgets linked to the organization's budget are all important elements of an IT strategic plan, but they do not necessarily leverage IT in achieving organizational goals. A comparison of future needs against current capabilities can help identify gaps and opportunities for improvement, but it does not provide a clear direction or roadmap for how to achieve them. A risk-based ranking of projects can help prioritize the most critical and beneficial projects, but it does not ensure that they are aligned with the business strategy or that they deliver value to the stakeholders. IT budgets linked to the organization's

budget can help allocate resources and monitor costs, but they do not reflect the impact or contribution of IT to the business performance or growth.
References:
Implement Agile IT Strategic Planning with Enterprise Architecture - The Open Group Blog
What is enterprise architecture? A framework for transformation | CIO Strategic Planning and Enterprise Architecture

NEW QUESTION: 393
□□ □ □□ □□ □□□□ □□ □ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □ □□?
A. □□□□□
B. FM-200
C. □□ □□□
D. □□
Answer: A (LEAVE A REPLY)
Carbon dioxide fire suppression systems need to be combined with an automatic switch to shut down the electricity supply in the event of activation. This is because carbon dioxide displaces oxygen in the air and can create a suffocation hazard for people in the protected area. Therefore, it is essential to cut off the power source before releasing carbon dioxide to avoid electrical shocks and sparks that could ignite the fire again.
Carbon dioxide systems are typically used for total flooding applications in spaces that are not habitable, such as server rooms or data centers.

NEW QUESTION: 394
IS □□□□ □□□ □□ □□□ □□□ □□ □□□ □□□□ □□□□. □□ □ □□ □□ □□□□ □□□□□?
A. IT □□□ □□ □□ □ □□ □□□ □□□□□.
B. □□□□ □□ □□□ □□□□ □□ □□(NAT)□ □□□ □ □□□□.
C. □□ □□□ □□ □□□□ □□□□□.
D. □□□ □□ □□□ □□ □□□ □□□ □□□□.
Answer: (SHOW ANSWER)
This should result in a finding because it violates the best practice of setting rules for groups rather than users. According to one of the web search results1, using group permissions instead of individual permissions can simplify the management and maintenance of ACLs, reduce the risk of human errors, and ensure consistency and compliance. Individual permissions can create conflicts, confusion, and security gaps in the ACLs. Therefore, the IS auditor should report this as a finding and recommend using group permissions instead.

NEW QUESTION: 395

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

A. □□ □□ □□□ □□

B. □□□ □□□□□□ □□ □□□ □□□□.

C. □□□□□□ □□□□ □□ □□ □□

D. □□□□□ □□□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 396

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

A. □□□ □□□ □□□□ □□□ □□ □ □□ □□□□□.

B. □□ □□□ □□ □□ □□ □□□ □□□□□.

C. □□ □□□□ □□ □□□ □□□□ □□ □□□□□.

D. □□ □□ □□□ □□□ □□□□ □□□□□□□.

Answer: A (LEAVE A REPLY)

Comprehensive and Detailed Step-by-Step Explanation:

Conducting vulnerability assessmentsonly once per year, right before an audit,creates a false sense of securityandleaves systems exposedbetween assessments.

* Annual Testing Before Audit (Correct Answer - A)
* Risksundetected vulnerabilitiesfor extended periods.
* Example:A company only tests security before acompliance audit, allowingzero-day threatsto persist for months.
* Internal Team Conducting Assessments (Incorrect - B)
* Not ideal, butregular assessmentsare more critical.
* Focusing on Critical Systems (Incorrect - C)
* Not perfect, butbetter than no testing at all.
* Using Open-Source Tools (Incorrect - D)
* Open-source toolscan be effective ifproperly configured.

References:

* ISACA CISA Review Manual
* NIST 800-115 (Technical Guide to Security Testing)

NEW QUESTION: 397

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

A. □□□□ □□□ □□

B. □□ □□ □□

C. □□ □□ □□

D. □□□ □□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 398
□□□□□ □□ □□□□□ □□ □□□□ IS □□□□ □□ □□□ □□□ □□□□ □□ □□.
A. □□ □□□□□ □□ □□□.
B. □□ □□□□□ □□□ □□.
C. □□□ □□□ □□□ □□ □□.
D. □□ □□□□ □□□.
Answer: (SHOW ANSWER)
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: 399
□□□ □□□□□ □□ □□□ □□□ □ IS □□□□ □□ □□ □□□ □□□ □ □□□ □□□□□?
A. □□□□
B. □□□ □ □□□ □□□ □□□
C. □□□□□□□(BCP) □□□ □□
D. □□ □□ □ □□
Answer: (SHOW ANSWER)

The IS auditor's primary focus when evaluating an organization's offsite storage facility should be the adequacy of physical and environmental controls. Physical and environmental controls are essential to protect the offsite storage facility from unauthorized access, theft, fire, water damage, pests or other hazards that could compromise the integrity and availability of backup media. Shared facilities is something that the IS auditor should consider when evaluating the offsite storage facility, but it is not the primary focus. Results of business continuity plan (BCP) test or retention policy and period are things that the IS auditor should review when evaluating the organization's BCP or backup strategy, not the offsite storage facility itself. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 388

NEW QUESTION: 400
□□□ □□□□□ □□□□ □□□□□□ □□□ □□□□ 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: 401
□□□ □□ □□ □□□□□ □□□□ IS □□□□ □□ □□□□ □□□□ □ □□□ □ □□□□?
A. □□□ □□□ □□□□ □□ □□□□□ □□□□ □□□□□ □□□□.
B. □□□ □□ □□ □□□□ □□□□□.
C. □□ □ □□ □□□ □□□□ □□ □□□ □□□□□□□.
D. □□□ □□□□ □□ □□□ □□□□ □□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 402
□□ □□□□ □□ □□□ □□□□ □□ □ □□□ □□□□□?
A. □□□□□ □ □□ □□ □□ □□ □□□ □□□□□.
B. □□□□ □□□□ □ □□□□□ □□□□□.
C. □□ □□□ □□□□□□□ □□ □□□□ □□□□ □ □□□□.
D. □□□ □□□□□ □□□ □□ □□□ □□□□□ □□□□ □ □□□□.

Answer: (SHOW ANSWER)
The greatest advantage of vulnerability scanning over penetration testing is that the testing process can be automated to cover large groups of assets. Vulnerability scanning is an automated, high-level security test that reports its findings of known vulnerabilities in systems, networks, applications, and devices. Vulnerability scanning can be performed frequently, quickly, and efficiently to scan a large number of assets and identify potential weaknesses that need to be addressed. Vulnerability scanning can also help organizations comply with security standards and regulations, such as PCI DSS1.
The other options are not as advantageous as option D, as they may not reflect the true benefits or limitations of vulnerability scanning compared to penetration testing. The testing produces a lower number of false positive results, but this is not necessarily true, as vulnerability scanning may report vulnerabilities that are not exploitable or relevant in the context of the organization. Network bandwidth is utilized more efficiently, but this may not be a significant advantage, as vulnerability scanning may still consume considerable network resources depending on the scope and frequency of the scans. Custom-developed applications can be tested more accurately, but this is also not true, as vulnerability scanning may not be able to detect complex or unknown vulnerabilities that require manual analysis or exploitation.
References:
* 1: Vulnerability scanning vs penetration testing: What's the difference? | TechRepublic
* 2: Vulnerability Scanning vs. Penetration Testing - Fortinet
* 3: Penetration Test Vs Vulnerability Scan | Digital Defense
* 4: Penetration Testing vs. Vulnerability Scanning: What's the difference?
* 5: Penetration Testing vs. Vulnerability Scanning | Secureworks
* 6: PCI DSS Quick Reference Guide - PCI Security Standards Council

NEW QUESTION: 403
□□ □□□□□ □□□□ □□□□ □□□ □□ □□□□ □□□ 60%□ □□□□□□ □ □□□□□. □□ □□□□ □□ □ □□□ □□ □□ □□□?
A. □□□ □□□ □□□ □□□□□.
B. □□□ □□□□ □□ □□ □□□□ □□□□□.
C. □□□□□□ □□
D. □□ □□ □□
Answer: A (LEAVE A REPLY)
The first thing that the audit manager should do when faced with a situation where only 60% of the audit has been completed and the due date is approaching is to determine where delays have occurred. This can help the audit manager to identify and analyze the root causes of the delays, such as unexpected issues, scope changes, resource constraints, communication problems, etc., and evaluate their impact on the audit objectives, scope, quality, and timeline. Based on this analysis, the audit manager can then decide on the best course of action to address the delays and complete the audit

successfully. Assigning additional resources to supplement the audit is a possible option for resolving delays in an audit project, but it is not the first thing that the audit manager should do, as it may not be feasible or effective depending on the availability, cost, and suitability of the additional resources. Escalating to the audit committee is a possible option for communicating delays in an audit project and seeking guidance or support from senior management, but it is not the first thing that the audit manager should do, as it may not be necessary or appropriate depending on the severity and urgency of the delays. Extending the audit deadline is a possible option for accommodating delays in an audit project and ensuring sufficient time for completing the audit tasks and activities, but it is not the first thing that the audit manager should do, as it may not be possible or desirable depending on the contractual obligations, stakeholder expectations, and regulatory requirements.

NEW QUESTION: 404
□□□ □□ □□□□ □□□ □□□ □□ □□ □□ □□□ □□□□□□□. □□ □ □□ □□□□ □□ □□□ □□□□□?
A. □□□□ □□□□ □□□ □□□ □□□ □□□□□ □□ □□□□.
B. IT□ □□□□□ □□ □□ □□□ □□ □□ □□□ □□□□□.
C. □□ □□□□□ □□□□ □□□□ □ □□□ □ □□□□□.
D. IT □□ □□ □□□ □□ □□□□ □□□ □□□ □□□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 405
□□□□ □□ □ □ □□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□ □ □ □□□ □□□□ □□□ □□□□. □ □□, □□□ □□ □□□ □ □□ □□□ □□ □ □ □□□ □□□□ □□□□□□. □□ □□ □□□ □□□□□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 406
□□□ □□□ □□ IT □□□□□ □□□□□ □□□□ □□ □□ □□□ □□□ □ IS □ □□□□ □□ □□□ □□ □□ □ □□□□□?
A. IT □□ □□
B. □□□ □□
C. IT □□ □□□
D. □□□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 407
□□ □□□ □□□ □□ □□□□ □□□ □□□ □□□□ □□□□□ □□□□ □□□ □ □ □□□□□□ □□□□ □□□ □□□□□□. □□ □ IS □□□□ □□□ □□ □□ □ □□□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□□ □□□□ □□□□□.
C. □□ □□ □□□ □□□ □□ □□□□□ □□□□□.
D. □□ □□ □□(CSA) □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 408
□□ □□ □□ □□(QA) □ □□□ □□ □□□□□ □□□□ □□ □□ □ □□ □ □□ □□□ □□□□□?
A. □□ □□□□□□ □□ □□□□□ □□□ □□□ □□□□ □□□□.
B. □□ □□□□ □□□□□□ □□□□ □□□□.
C. □□ □□ □□□ □□□□ □□□□ □□□□.
D. □□ □□□ □□ □□□□□ □□□ □□□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
According to the ISACA CISA documentation, one of the requirements for internal audit quality assurance (QA) and continuous improvement processes is to have an external assessment at least once every five years by a qualified, independent reviewer or review team from outside the organization1. This is to ensure that the internal audit activity conforms to the International Standards for the Professional Practice of Internal Auditing (the Standards) and the Code of Ethics, and to identify opportunities for improvement2. Therefore, the lack of periodic engagement with external assessors would present the greatest concern during a review of internal audit QA and continuous improvement processes.

NEW QUESTION: 409
□□□ □□ □□□ □□ □□□ □□□□ □□ IS □□□ □□□□□ □□ □□□ □□□ □□□□ □□□.
A. □□ □□ □□(DRP) □□ □□□ □□□□□.
B. □□□□ □□□□□ □□ □□ □□□ □□□□□.
C. □□ □□ □□□ □3□□□ □□□□□.

D. □□ □□ □□□ □□ □□□ □□

Answer: B (LEAVE A REPLY)

An organization outsourced its IS functions. To meet its responsibility for disaster recovery, the organization should coordinate disaster recovery administration with the outsourcing vendor. This is because the organization remains accountable for ensuring the continuity and availability of its IS functions, even if they are outsourced to a third party. The organization should establish clear roles and responsibilities, communication channels, testing procedures, and escalation processes with the outsourcing vendor for disaster recovery purposes. The organization should not discontinue maintenance of the disaster recovery plan (DRP), as it still needs to have a documented and updated plan for restoring its IS functions in case of a disaster. The organization should not delegate evaluation of disaster recovery to a third party or internal audit, as it still needs to monitor and review the performance and compliance of the outsourcing vendor with respect to disaster recovery objectives and standards. References: CISA Review Manual (Digital Version), [ISACA Auditing Standards]

NEW QUESTION: 410

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

A. □□

B. □□□

C. □□□

D. □□

Answer: (SHOW ANSWER)

Comprehensive and Detailed Step-by-Step Explanation:

Minimizing business downtime is critical when implementing a new system that supports an essential process like month-end closing.

* Option A (Incorrect):Thebig bang approachinvolves replacing the old system with the new system all at once. This method carries ahigh riskbecause if issues arise, they may causesignificant downtime and disruption.
* Option B (Correct):Aphased approachgradually implements the system in stages, allowing users to adaptand minimizing the risk of complete failure. This strategy is ideal for critical systems that cannot afford extended downtime.
* Option C (Incorrect):Thecutover approachis a variation of big bang, where the old system is shut down, and the new system is activated. This method isriskyfor month-end processes because errors can causebusiness delays.
* Option D (Incorrect):Theparallel approachruns both old and new systems simultaneously to verify accuracy, but it isresource-intensiveand may not be practical for a high-volume month-end process.

Reference:ISACA CISA Review Manual -Domain 3: Information Systems Acquisition, Development, and Implementation- Covers system implementation strategies, risk management, and best practices.

NEW QUESTION: 411
□□ □ □□□ □□□ □□□ □□ □□□ □□□□ □□ □□□□ □□ □□□ □□□□ □?
A. □□ □□ □□□ □□ □□
B. □□□ □□ □□□ □□□ □□□□
C. □□ □□ □□
D. □□□□ □□ □□
Answer: C (LEAVE A REPLY)
The most effective control to mitigate unintentional misuse of authorized access is security awareness training. This is because security awareness training can educate users on the proper use of their access rights, the potential consequences of misuse, and the best practices to protect the confidentiality, integrity, and availability of information systems. Security awareness training can also help users recognize and avoid common threats such as phishing, malware, and social engineering.
Annual sign-off of acceptable use policy, regular monitoring of user access logs, and formalized disciplinary action are not the most effective controls to mitigate unintentional misuse of authorized access. These controls may help deter or detect intentional misuse, but they do not address the root cause of unintentional misuse, which is often a lack of knowledge or awareness of security policies and procedures.

NEW QUESTION: 412
IT □□ □□□□ □□□□ □□ □□□□□ □□□□ □□ □□□ □□□ □□□□ □□ □ □ □□□ □□□□□. □ □□ □□□ □□□ □□ □□□ □□□ □□□□□?
A. □□□□ □□□
B. IT □□ □□□
C. □□□□ □□□
D. □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 413
□□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□ □□ □□ □□ □□□ □□□ □ □□□□.
A. □□ □□.
B. □□ □□.
C. □□.
D. □□ □□.
Answer: (SHOW ANSWER)

Segregation of duties is a key internal control that aims to prevent fraud and errors by ensuring that no single individual has the authority to execute two or more conflicting sensitive transactions or functions. In the accounts payable vendor payment cycle, segregation of duties involves separating the tasks of vendor setup, procurement, invoice approval, and payment processing1. This way, an employee cannot create a fictitious vendor and issue a payment to themselves or their accomplices without being detected by another person. Therefore, the best way to prevent fraudulent payments is to implement segregation of duties between the vendorsetup and payment processing. References: 1: Segregation of Duties in the Accounts Payable Vendor Payment Cycle for SMBs - Now With a Podcast! - Debra R Richardson : What is Separation of duties
- University of California, Berkeley

NEW QUESTION: 414
IS □□□□ □□□□ □□□ □ □□ □□ □□□ □□ □□□?
□□ □□ □□ □□□□ □□ □□ □□ □□ □□□ □□□□□.
□□□ □ □□ □□□□□ □□□□?
A. □□□ □□ □□□ □□□□ □□□□□.
□□□□.
B. □□□□□ □□□□ □□□ □□□□□.
C. □□□ □ □□ □□□□□ □□ □□□□ □□□ □□□□□.
D. □□ □□ □□□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The first thing that an IS auditor should do when management responses to an in-person internal control questionnaire indicate a key internal control is no longer effective is to ascertain the existence of other compensating controls. Compensating controls are alternative controls that provide reasonable assurance of achieving the same objective as the original control. The IS auditor should verify whether there are any compensating controls in place that can mitigate the risk of the key control being ineffective, and evaluate their adequacy and effectiveness. The other options are not the first steps, because theyeither require more information about the compensating controls, or they are actions to be taken after identifying and assessing the compensating controls. References: CISA Review Manual (Digital Version)1, Chapter 2, Section 2.2.3

NEW QUESTION: 415
□□□ □□ □□□□ □□□□ 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: 416
□□ □□ □□□□ □□ □□□ □□□ □□□□.
A. □□□□□ □□□□□ □□□□□.
B. □□□□□□ □□□□ □□□□□.
C. □□□ □□□ □□□□□.
D. □□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
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: 417
IS □□□□ □□□□□ □□□ □□□□□□□ □□ □□□ □□□ □□□□□ □□□ □ □ □□□ □□ □□□□□.
□ □□□□ □□ □ □□ □□□ □□ □ □□□□□?
A. □□ □□ □□
B. □□□ □□ □□ □□□ □□□
C. □□ □ □□ □□(MTBF) □□
D. □□□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 418
IS □□□□ □□ □□□□ □□□□□□□ □□□ □ □□□ □□□□ □□ □□□ □□□ □ □□ □□□□ □□□□ □□□□. □□ □ □□□□ □□ □ □□ □□□ □□□□□?
A. □□□□□□ □□□ □□ □□□ □□□□□ □□□□ □□□□□.
B. □□ □□ □□□ IT □□□ □□□□ □□□□□.
C. □3□ □□□ □□□□□ □□□□ □□□□□.
D. □3□ □□□ □□□□ □□ □□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
The third-party contract has not been reviewed by the legal department is the auditor's greatest concern because it poses a significant legal and financial risk to the client. A third-party contract is a legally binding agreement between the client and the outsourced payroll provider that defines the scope, terms, and conditions of the service. A third-party contract should be reviewed by the legal department to ensure that it complies with the applicable laws and regulations, protects the client's interests and rights, and specifies the roles and responsibilities of both parties. A third-party contract that has not been reviewed by the legal department may contain clauses that are unfavorable, ambiguous, or contradictory to the client, such as:
Inadequate or unclear service level agreements (SLAs) that do not specify the quality, timeliness, and accuracy of the payroll service.
Insufficient or vague security and confidentiality provisions that do not safeguard the client's data and information from unauthorized access, use, disclosure, or loss.
Unreasonable or excessive fees, penalties, or liabilities that may impose an undue financial burden on the client.
Limited or no audit rights that may prevent the client from verifying the effectiveness and compliance of the payroll provider's internal controls.
Inflexible or restrictive termination clauses that may limit the client's ability to cancel or switch to another payroll provider.

A third-party contract that has not been reviewed by the legal department may expose the client to various risks, such as:
Legal disputes or litigation with the payroll provider over contractual breaches or performance issues.
Regulatory fines or sanctions for noncompliance with tax, labor, or other laws and regulations related to payroll.
Financial losses or damages due to errors, fraud, or negligence by the payroll provider.
Reputation damage or customer dissatisfaction due to payroll errors or delays.
Therefore, an IS auditor should be highly concerned about a third-party contract that has not been reviewed by the legal department and recommend that the client seek legal advice before signing or renewing any contract with an outsourced payroll provider.
User access rights have not been periodically reviewed by the client is a moderate concern because it may indicate a lack of proper access control over the payroll system. User access rights are the permissions granted to users to access, view, modify, or delete data and information in the payroll system. User access rights should be periodically reviewed by the client to ensure that they are aligned with the user's roles and responsibilities, and that they are revoked or modified when a user changes roles or leaves the organization. User access rights that are not periodically reviewed by the client may result in unauthorized or inappropriate access to payroll data and information, which may compromise its confidentiality, integrity, and availability.
Payroll processing costs have not been included in the IT budget is a minor concern because it may indicate a lack of proper planning and allocation of IT resources for payroll processing. Payroll processing costs are the expenses incurred by the client for using an outsourced payroll service, such as fees, charges, taxes, or penalties. Payroll processing costs should be included in the IT budget to ensure that they are adequately estimated, monitored, and controlled. Payroll processing costs that are not included in the IT budget may result in unexpected or excessive costs for payroll processing, which may affect the client's profitability and cash flow.
The third-party contract does not comply with the vendor management policy is a low concern because it may indicate a lack of alignment between the client's vendor management policy and its actual vendor selection and evaluation process. A vendor management policy is a set of guidelines and procedures that governs how the client manages its relationship with its vendors, such as how to select, monitor, evaluate, and terminate vendors. A vendor management policy should be consistent with the client's business objectives, risk appetite, and regulatory requirements. A third-party contract that does not comply with the vendor management policy may result in suboptimal vendor performance or service quality, but it does not necessarily imply a breach of contract or a violation of law.

NEW QUESTION: 419

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

A. □□ □□□ □□

B. □3□□ □□ □□ □□

C. □ □□□□□□ □□□(WAF) □□

D. □□□□□□ □□□□□□ □□□□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 420

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

A. □□ □□ □ □□□□ □□

B. □□ □□□□□ □ □□□□□

C. □□□□ □□□

D. □□ □□ □□

Answer: A (LEAVE A REPLY)

A network vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the network or its resources. A network vulnerability assessment typically involves scanning the network devices, such as routers, switches, firewalls, servers, and workstations, using automated tools that compare the device configurations, software versions, and patch levels against a database of known vulnerabilities. A network vulnerability assessment can also include manual testing and verification of the network architecture, design, policies, and procedures. One of the main objectives of a network vulnerability assessment is to detect and report any misconfiguration and missing updates in the network devices that could pose a security risk1.

Misconfiguration refers to any deviation from the recommended or best practice settings for the network devices, such as weak passwords, open ports, unnecessary services, default accounts, or incorrect permissions. Missing updates refer toany outdated or unsupported software or firmware that has not been patched with the latest security fixes or enhancements from the vendors2. Misconfiguration and missing updates are common sources of network vulnerabilities that can be exploited by attackers to gain unauthorized access, executemalicious code, causedenial of service, or escalate privileges on the network devices3.

Therefore, an IS auditor should expect to see misconfiguration and missing updates in a network vulnerability assessment. The other options are less relevant or incorrect because:

* B. Malicious software and spyware are not usually detected by a network vulnerability assessment, as they are more related to the content and behavior of the network traffic rather than the configuration and patch level of the network devices. Malicious software and spyware are programs that infect or monitor the network devices or their users for malicious purposes, such as stealing data, displaying ads, or performing remote

commands. Malicious software and spyware can be detected by other security tools, such as antivirus software, firewalls, or intrusion detection systems4.
* C. Zero-day vulnerabilities are not usually detected by a network vulnerability assessment, as they are unknown or undisclosed vulnerabilities that have not been reported or patched by the vendors or the security community. Zero-day vulnerabilities are rare and difficult to discover, as they require advanced techniques and skills to exploit them. Zero-day vulnerabilities can be detected by other security tools, such as intrusion prevention systems, anomaly detection systems, or artificial intelligence systems5.
* D. Security design flaws are not usually detected by a network vulnerability assessment, as they are more related to the logic and functionality of the network rather than the configuration and patch level of the network devices. Security design flaws are errors or weaknesses in the network architecture, design, policies, or procedures that could compromise the security objectives of the network. Securitydesign flaws can be detected by other security methods, such as security reviews, audits, or assessments6. References: Network VulnerabilityAssessment - ISACA, Network Vulnerability Scanning - NIST, Network Vulnerabilities - SANS, Malware - ISACA, Zero-Day Attacks
- ISACA, Security Design Principles - NIST

NEW QUESTION: 421
□□□, □□, □□ □□□(IoT) □□□ □□ Zero Trust □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□□□□ □□□□□ □□□□□ □□□□□.
B. □□□□ □□ □□□□ □□□□ □□ □□ □□ □ □□□□ □□□ □□□□□.
C. □□ □□ □□□ □□ □□□ □□ □ □□ □□□ □□
D. □□ □ □ □□ □□ □□□□ □□ □□□ □□□ □□□□ □□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Zero Trustis based on the principle of"never trust, always verify,"makingidentity validationthe most critical aspect.
* Option A (Incorrect):Firmware updatesare important for security but are onlyone partof aZero Trustapproach.
* Option B (Correct):Device and user identity validationensures that onlyauthorizedentities can accesscritical resources, reducing the risk of unauthorized access.
* Option C (Incorrect):User awarenessis important but does not enforce access control, which isfundamentalto Zero Trust.
* Option D (Incorrect):Encryptionsecures data but does not controlwho can access resources, which is the primary focus of Zero Trust.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-CoversZero Trust security models and access control best practices.

NEW QUESTION: 422
IS □□□□ □□ □□□□ □□□□ IT □□□ □□ □□□□□□ □□□ □□□□□ □□ □□ □□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□□□. □□ □ □□ □□ □□□□ □□□ □□□□ □□□□ □□□□ □ □□□□ □□ □□□ □□ □□□ □□□ □ □□□□□ □ □□ □□□ □□□?
A. □□□□ □□
B. □□□ □□ □□
C. IT □□□□ □□□□□
D. □□□□□ □□
Answer: (SHOW ANSWER)
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: 423
□□ □□□ □□□ □□□□ □□ □□ □□(B1A)□ □□□ □ □□□□ □ □□ □□□ □ □□ □□□□□?
A. □□ □□□
B. □□□□□ □□□ □□□□□□
C. □□ □□ □□□□□ □□□
D. □□ □□□□
Answer: C (LEAVE A REPLY)
The most important thing to assess when conducting a business impact analysis (BIA) is the completeness of critical asset inventory. This is because the critical asset inventory is the basis for identifying and prioritizing the business processes, functions, and resources that are essential for thecontinuity of operations. The critical asset inventory should include

both tangible and intangible assets, such as hardware, software, data, personnel, facilities, contracts, and reputation. The critical asset inventory should also be updated regularly to reflect any changes in the business environment or needs. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.41
* CISA Online Review Course, Domain 3, Module 3, Lesson 12

NEW QUESTION: 424
IS □□□□ □□ □□ □□□ □□ □□□ □□, □□□□ □□ □□□ □□□□ □□ □□ □ □□□□□□.
IS □□□□ □□ □□□ □□ □ □□□□□ □□□?
A. □□□□ □□ □□□ □□□ □□□ □□□ □ □□□□□□ □□□ □□□ □□□□□ □.
B. □□ □□ □□□ □□□□ □□ □□ □□□□ □□□□□.
C. □□ □□□ □□ □□□ □□□ □□□□□.
D. □□ □□□ □□□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□□□□□.
Answer: D (LEAVE A REPLY)
If an IS auditor finds that management did not address a prior period audit finding, the next course of action should be to interview management to determine why the finding was not addressed, as this would help to understand the root cause, the impact, and the risk level of the issue. Noting the exception in a new report, recommending alternative solutions, or conducting a risk assessment are possible subsequent steps, but they should not precede interviewing management. References: CISA Review Manual (Digital Version), Chapter 1, Section 1.6

NEW QUESTION: 425
□□ □ □□□□ □□□ □□ □□□ □□□□□ □□□□□□ □□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□□ □□□□□ □□
B. □□ □□ □□
C. □□ □□ □□
D. □□ □□□ □□
Answer: C (LEAVE A REPLY)
The best audit evidence that a firewall is configured in compliance with the organization's security policy is to review the rule base. The rule base is a set of rules that defines the criteria for allowing or denying network traffic through the firewall. By reviewing the rule base, the auditor can verify if the firewall configuration matches the security policy requirements and objectives. Analyzing how the configuration changes are performed, analyzing log files, and performing penetration testingare useful audit techniques, but they do not provide direct evidence of the firewall configuration compliance. References: CISA Review Manual (Digital Version)1, page 383.

NEW QUESTION: 426
IS □□□□ □□□ □□□ □□ □□ □□(SDLC)□ □□□□ □□□□. □□ □ □□ □□ □ □□□ □□□ □□□□□ □□□?
A. □□□ □□ □□ □□□ □□□
B. □□□ □□ □□□□□ □□ □□□ □□□□□ □□
C. □□□ □□ □□□□ □ □□□□ □□ □□
D. □□□□ □□□ □□ □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 427
□□ □□□ □□□ □□ □□□□ □□□□ □□□ □□□□ □□□ □□ □□□□ □□□ □ □□□□□?
A. □□
B. □□
C. □□
D. □□□
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Exploitationis the phase where testersleverage identified vulnerabilitiestogain unauthorized accessto systems.
* Exploitation (Correct Answer - B)
* Attackers use techniques such as SQL injection, buffer overflow, or privilege escalation.
* Example:A tester exploits a weak password to gain admin access.
* Exfiltration (Incorrect - A)
* The process of stealing dataaftergaining access.
* Reconnaissance (Incorrect - C)
* The initial stage where attackers gather information about the target.
* Scanning (Incorrect - D)
* Involves identifying open ports and services but does not involve actual attacks.
References:
* ISACA CISA Review Manual
* NIST 800-115 (Technical Guide to Security Testing)

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

The first action that an IS auditor should take when finding a high-risk vulnerability in a public-facing web server used to process online customer payments is to identify compensating controls. Compensating controls are alternative or additional controls that provide reasonable assurance of mitigating the risk of exploiting the vulnerability. The IS auditor should assess the effectiveness of the compensating controls and determine whether they reduce the risk to an acceptable level. If not, the IS auditor should recommend remediation actions to address the vulnerability. Documenting the exception in an audit report is an important action, but it should not be the first action, as it does not address the urgency of the situation. Reviewing security incident reports is a useful action, but it should not be the first action, as it does not provide assurance of preventing future incidents. Notifying the audit committee is a necessary action, but it should not be the first action, as it does not involve taking any corrective measures. References:
* CISA Review Manual, 27th Edition, pages 295-2961
* CISA Review Questions, Answers & Explanations Database, Question ID: 260

NEW QUESTION: 429
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: 430
□□□□ □□ □□ □□□ □□ □□□ □□ □□ □□□□ □□□ □ □□□ □□ □ □□ □□□ □□ □□□□□?

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: 431
□ □□□□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□□ □□ □□□□ □□ □□ □□□ □□□□□□ □□□□□ □□□□□□.
□□ □ □□□□ □□□□□ □□□□ □ □□□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□ □□□□ □□□ □□ □□ □□□ □□ □□□□□ □□ □□□□ □□□□.
B. □□ □□□□ □□□□□□□□□□ □□□□ □□ □□□□□ □□□□□.
C. □□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□ □□ □□□□ □□□□ □ □□□.
D. □□ □□□ □□□ □□□ □□□□ □□ □□□□□□□□□□ □□ □□□□ □□□ □□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 432
□□ □ □□□□ □□ □□□ □□□ □□ □□□ ST □□□ □□ □□ □□□□□?
A. □□ □□□□ □□ □□ □□ □□□□□□.
B. □□ □□ □□□ □□□ □□
C. □□ □□ □□ □□
D. □□□ □□ □□□ □□ □□ □□
Answer: A (LEAVE A REPLY)
The greatest impact as a result of the ongoing deterioration of a detective control is an increased number of false negatives in security logs. A detective control is a control that monitors and identifies any deviations or anomalies from the expected or normal behavior

or performance of a system or process. A security log is a record of events or activities that occur within a system or network, such as user access, file changes, system errors, or security incidents. A false negative is a situation where a security log fails to detect or report an actual deviation or anomaly that has occurred, such as an unauthorized access, a malicious modification, or a security breach. An increased number of false negatives in security logs can have a significant impact on the organization's security posture and risk management, because it can prevent timely detection and response to security threats, compromise the accuracy and reliability of security monitoring and reporting, and undermine the accountability and auditability of user actions and transactions. The other options are not as impactful as anincreased number of false negatives in security logs, because they either do not affect the detection capability of a detective control, or they have less severe consequences for security management. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.1

NEW QUESTION: 433
IS □□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□. □□□ □□□ □□□□ □□□ □ □□□□ □□ □□□□ □□□ □□ □□□ □ □ □□□ □□ □□□□ □□□□□ □□□?
A. □□□ □□□
B. □□□□ □□
C. □□ □□□
D. □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 434
□□ □□ □□ IS □□ □□□□ □□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □□□ □□□□ □□□□. □ □□□□ □□ □ □□ □□ □□ □□□ □ □□□□?
A. □□□□ □□ □□□ □□ □□ □□□ □□□□□ □□□□□□□.
B. □□□ □□ □□□□ □□ □□□ □□□ □□□ □□□□□.
C. □□□ □□□ □□□ □□□□ □□□□ □□□ □□□□□.
D. □□ □□□ □□□ □□□□ □□□ □□□ □□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)
Audit planning is the process of developing an overall strategy and approach for conducting an audit. Audit planning involves identifying the objectives, scope, criteria, and methodology of the audit, as well as the resources, schedule, and reporting requirements. Audit planning also involves performing a risk assessment to identify and prioritize the areas of highest risk and significance for the audit1.
Risk assessment is a systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking. Risk assessment involves identifying the

sources and causes of risk, analyzing the likelihood and impact of risk, and determining the level of risk and the appropriate response2.
During audit planning, the IS audit manager is considering whether to budget for audits of entities regarded by the business as having low risk. The best course of action in this situation is C. Validate the low-risk entity ratings and apply professional judgment.
This is because validating the low-risk entity ratings can help to ensure that the risk assessment is accurate, reliable, and consistent with the business objectives and expectations. Validating the low-risk entity ratings can also help to identify any changes or developments that may affect the risk profile of the entities since the last assessment. Applying professional judgment can help to determine whether the low-risk entities should be included or excluded from the audit plan, based on factors such as materiality, relevance, significance, and assurance needs3.

NEW QUESTION: 435
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: 436
IT □□ □□□ □□□ □ IS □□□□ □□ □□□ □□□□□ □□□ □□□□ □□□.
A. IT □□ □□.
B. □□□ □□□□ □□ □□□.

C. □□ IT □□□□□.
D. □□ □□ □□□ □□ □□.
Answer: (SHOW ANSWER)
In reviewing the IT strategic plan, the IS auditor should consider whether it identifies the major IT initiatives that are aligned with the organization's vision, mission, and objectives, and that support the business strategy and priorities12. The major IT initiatives should also be realistic, measurable, and achievable, and should have clear timelines, budgets, and responsibilities34.
References
1: IT Strategy Template for a Successful Strategic Plan | Gartner2 2: IT Strategy Template for a Successful Strategic Plan | Gartner4 3: Conduct a Strategic Plan Review & Assessment - Governance3 4: Time To Conduct A Strategy Review? Here's How To Get Started1

NEW QUESTION: 437
□□□ □□□ □□□□ □ □□ □□□ □□□□ □□ □□ □□ □ □□ □□ □□□ □□ □?
A. □□ □□□
B. □□□ □□ □□(DLP) □□□
C. □ □□□□□□ □□□
D. □□□□ □□□
Answer: D (LEAVE A REPLY)
Network segmentation is the best security measure to reduce the risk of propagation when a cyberattack occurs, because it divides the network into smaller subnetworks that are isolated from each other and have different access controls and security policies. This limits the spread of malicious traffic and prevents attackers from accessing sensitive data or systems in other segments. Aperimeter firewall, a data loss prevention (DLP) system, and a web application firewall are also useful security measures, but they do not prevent propagation within the network as effectively as network segmentation does. References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.3

NEW QUESTION: 438
□□□□ □□ □□□□ □□□ □ □□ □ □□ □□□□□ □□□□ □□□?

A. □□□ □□□□□ □□□□(UDP)
B. □□□□□□ □□ □□□□(HTTP)
C. □□ □□ □□ □□□□(SFTP)
D. □□ □□□□ □□□□(RDP)
Answer: C (LEAVE A REPLY)
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: 439
□□ □ □□□ □□□ □□ □ □□ □□□ □□ □□□□ □□□□ □ □□ □□□□□?
A. □□□ □□□ □□ □□
B. □□□ □□□ □□
C. □□ □□ □□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)
The most important thing to include in forensic data collection and preservation procedures is preserving data integrity. Data integrity is the property that ensures that data is accurate, complete, and consistent throughout its lifecycle. Preserving data integrity is essential for forensic data collection and preservation procedures because it ensures that the data can be used as valid and reliable evidence in legal proceedings or investigations. Preserving data integrity can be achieved by using methods such as hashing, checksums, digital signatures, write blockers, tamper-evident seals, or timestamps. The other options are not as important as preserving data integrity in forensic data collection and preservation procedures, as they do not affect the validity or reliability of the data. Assuring the physical security of devices is a security measure that protects devices from unauthorized access, theft, damage, or destruction, but it does not ensure that the data on the devices is

accurate, complete, and consistent. Maintaining chain of custody is a documentation technique that records and tracks the handling and transfer of devices or data among different parties involved in forensic activities, but it does not ensure that the data on the devices is accurate, complete, and consistent. Determining tools to be used is a planning activity that selects and prepares the appropriate tools for forensic data collection and preservation procedures, but it does not ensure that the data collected and preserved by the tools is accurate, complete, and consistent. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.4

NEW QUESTION: 440
□□□ ERP(Enterprise Resource Planning) □□□□□□ □□□□□□ □□□ □ IS □□ □□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□□□ □ □□ □ □□□ □□□□□□□□.
B. □□ □□□ □ □□□ □□□□ □□□□□□□.
C. □□□□□□ □□□ □□□ □□ □□ □□□ □□□□□□□.
D. □ □□□ □□ □□□ □□□□ □□ □□□□□□ □□ □□□ □□□□□□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 441
□□ □ □□ □□ □□□ □□ □□ □□ □□□ □□□ □□□ □□□□ □ □□ □□□□ □?
A. □□□ □□ □□ □□□ □□□□□ □□
B. □□□□ □□□□□ □□ □□□□ □□ □□ □□□□□ □□
C. □□□ □□ □□ □□□□ □□□□ □□□ ID□ □□□ □□□□□.
D. □□□ □□ □□□□ □□ □□□□ □□ □□
Answer: D (LEAVE A REPLY)
Restricting program functionality according to user security profiles is the best control for ensuring appropriate segregation of duties within an accounts payable department. An IS auditor should verify that the access rights and permissions of the accounts payable staff are based on their roles and responsibilities, and that they are not able to perform incompatible or conflicting functions such as creating, approving, or paying invoices. This will help to prevent fraud, errors, or abuse of authority within the accounts payable process.
The other options are less effective controls for ensuring segregation of duties, as they may involve audit trails, access restrictions, or user identification. References:
* CISA Review Manual (Digital Version), Chapter 6, Section 6.31
* CISA Review Questions, Answers & Explanations Database, Question ID 223

NEW QUESTION: 442
□□ □ □□□ □□ □□ □□□□□ □□□ □□ □ □□□□ □□ □□□□□?
A. □□□ □□□ □□□□□□□.

B. □□ □□□ □□□□□□.
C. □□ □□□ □□□□□□.
D. □□□□ □□□ □□□□□□.
Answer: B (LEAVE A REPLY)
The effectiveness of a risk management program can be measured by how well it reduces the residual risk, which is the risk that remains after applying controls, to an acceptable level. Inherent risk is the risk that exists before applying any controls, and it cannot be eliminated completely. Control risk is the risk that the controls fail to prevent or detect a risk event, and it is a component of residual risk. Overall risk is not a meaningful metric for assessing the effectiveness of a risk management program, as it does not account for the impact and likelihood of different risk events. References: CISA Review Manual (Digital Version), Chapter 1, Section
1.2.2

NEW QUESTION: 443
□□□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□□□. □□ □ IS □□□□□ □□ □ □□□□ □□□□□?
A. □□□□ □□□ □□□□□ □□□ □□□□ □□□□□.
B. □□□□ □□□□□ □□ □□□ □□□ □□□ □□□□□.
C. □□□□ □□ □□□□□□ □□ □□□□ □□□ □ □□□□.
D. □□□□□ □□ □ □ □ □□ □□□□ □□□□ □□□□□□□.
Answer: B (LEAVE A REPLY)
The greatest concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users is that the survey questions did not address the scope of the business case. A post-implementation review is a process of evaluating the outcomes and benefits of a project after it has been completed and implemented. A post-implementation review can help to assess whether the project met its objectives, delivered its expected value, and satisfied its stakeholders1. A survey is a method of collecting feedback and opinions from users or other stakeholders about their experience and satisfaction with the project. A survey can help to measure the user acceptance, usability, and functionality of the project deliverables2. A business case is a document that justifies the need for a project based on its expected benefits, costs, risks, and alternatives. A business case defines the scope, objectives, and requirements of the project and provides a basis for its approval and initiation3. Therefore, an IS auditor should be concerned if the survey questions did not address the scope of the business case, as it may indicate that the post-implementation review was not comprehensive, relevant, or aligned with the project goals.
The other options are less concerning or incorrect because:
* A. The survey results were not presented in detail to management is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a communication or reporting issue than an audit issue. While presenting the survey results in detail to management may help to inform them about the

project performance and outcomes, it does not affect the validity or quality of the post-implementation review itself.
* C. The survey form template did not allow additional feedback to be provided is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a design or format issue than an audit issue. While allowing additional feedback to be provided may help to capture more insights or suggestions from users, it does not affect the validity or quality of the post-implementation review itself.
* D. The survey was issued to employees a month after implementation is not a great concern for an IS auditor when a post-implementation review was conducted by issuing a survey to users, as it is more of a timing or scheduling issue than an audit issue. While issuing the survey to employees sooner after implementation may help to collect more accurate and timely feedback from users, it does not affect the validity or quality of the post-implementation review itself. References: Post Implementation Review - ISACA, Survey - ISACA, Business Case - ISACA

NEW QUESTION: 444
□□ □□ □□ □□ IS □□□□ □□ □□□□□ □□□□□ □□□□ □□ □□□□□ □.
□□□□ □□□□□ □□□□ □□□ □ □□□ □□□□□. □□□□ □□□ □□ □□□ □□ □ □□ □□□□?
A. □□ □ □□□□ □□□□ □□□ □□□□ □□□□ □□□□□.
B. □□ □□ □□□□ □□□ □□□□ □□□□ □□□□□ □□□□.
C. □□ □□□□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□□□.
D. □□□□ □□□□□ □□ □□□ □□□□ □□□ □□□□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 445
□□ □ □□ □□ □□□(IDS)□ □□ □□□ □□□□□?
A. □□□ □□□□ □□ □□ □□
B. □□ □□□□ □□□ □□
C. □□ □□□ □□□□□ □□□ □ □□
D. □□□ □□ □□□ □□□ □ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 446
□□ □□ □□□ □□ □□□□ IS □□□□ □□□ □□ □□ □□ □□ □□□□□ □□ □ □□ □□□ □□□ □□ □□ □□ □□□ □□□□ □□□□ □□ □□□□□. □□□ □ □□ □□□ □□ □□□?
A. □□□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□ □□□□□.

C. □□□ □□ □□□□□ □□□□□□□(CIO)□□ □□□□□.
D. □□□ □□ □□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
Asking management why the regulatory changes have not been included is the first thing that an IS auditor should do during the planning stage of a compliance audit. An IS auditor should inquire about the reasons for not updating the inventory of compliance requirements with recent regulatory changes related to managing data risk. This will help the IS auditor to understand whether there is a gap in awareness, communication, or implementation of compliance obligations within the organization. The other options are not the first things that an IS auditor should do, but rather possible subsequent actions that may depend on management's response. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.31
* CISA Review Questions, Answers & Explanations Database, Question ID 214

NEW QUESTION: 447
□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□ □ □□ □□□ □□ □□ □□ □□□ □□□□ □□ □□ □□□ □□ □ □□□□□?
A. □□□ □□□ □□□ □□□□ □□□□□.
B. □□□ □□□□□ □□□ □□□□ □□ □□ □□□ □□□□□.
C. □□□□□ □□□ □□□
□□□ □□□□□ □□□ □□□□□.
D. □□ □□□ □□□ □□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Limiting the use of logs to only those purposes for which they were collected is the best way to address potential data privacy concerns associated with inadvertent disclosure of machine identifier information contained within security logs, because it minimizes the risk of unauthorized access, misuse, or leakage of personal data that may be embedded in the logs. Logs should be collected and processed in accordance with the data protection principles and regulations, such as theGeneral Data Protection Regulation (GDPR)
12. Restricting the transfer of log files from host machine to online storage, only collecting logs from servers classified as business critical, and limiting log collection toonly periods of increased security activity are not effective ways to address data privacy concerns, because they do not prevent or mitigate the potential disclosure of personal datain the logs. References: 1: CISA Review Manual (DigitalVersion), Chapter 5, Section 5.4.4 2: CISA Online Review Course, Module 5, Lesson 4

NEW QUESTION: 448
IS □□□□ □□ □□□ □□ □□ □□ □□□□ □□ □□□□ □□□□ □□□, □□□ □□ □□□ □□□□□ □□ □□□ □□□ □□□□ □□□□. □□□□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □ □□□□□?
A. □□□□ □□□ □ □□□ □□□ □□□

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

NEW QUESTION: 449
□□ □□□□□ □□ □□□ □□□ □□□ □□□ □□□ □□ □□□□□ □□ □□ □ □□□.
A. □□ □□ □□□□ □□ □□□ □□□□□□ □□ □□□ □□□□□.
B. □□ □□□ □□□□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□□.
C. □ □□□□□ □□□□ □□ □□□ □□□□□□.
D. □□□□□□ □□□ □□ □□□ □□ □□ □□□□□.
Answer: (SHOW ANSWER)
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: 450
□□□ □□ □□ □□(DRP)□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □ □□□□?
A. DRP□ □□ □□ □□□□ □□ □□□ □□ □□□□□.
B. DRP□ □□ □□□□□ □□□□ □□□□□.
C. IT □□□ □□□□□ □□ DRP□ □□□□□□ □□□□□.
D. DRP□□ □□□ □□□ □□ □□ □□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
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: 451
□□ □ □□□ □□□ □□□ □□□□□ □□ □□ □□□ □□□ □□□□□?
A. □□□□ □□
B. □□□□ □□□ □□ □□
C. □□ □□ □□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 453
□□ □ 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: 454
IS □□ □□□ IT □ □□□□ □□□□ □□□ □□ □□□ □□□□□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□. □□□ □□□ □□□□□ □□□□ □□ □□□ □□□□□□□. □□ □ □□ □ □□ □□□ □□□□□?
A. □□□ □□□ □□□ □□□
B. □□□ □□□ □□□ □□
C. □□□ □□□ □□□□ □□□□□□.
D. □□□ □□□ □□□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 455
IS □□□□ □□□ □□□□ □□ □□□□□ □□□ □□□□ □□□□. □□ □ □□□ □ □□ □ □□□□ □□ □□□□?
A. □□□□□ □□ □□□□ □□
B. □□□□□ □□ □ □□
C. □□□□□ □□ □□
D. □□□□□ □□ □□

Answer: D (LEAVE A REPLY)

NEW QUESTION: 456
□□□□□ □□ □□□ Enterprise Resource Planning(ERP) □□□□ □□ □□□ □□□ □□ □□□□ □□□□. □□ □□(QA) □□ □ □□ □ □□ □□□□ □ □□□ □□□□ □□?
A. □□□□
B. □□
C. □□
D. □□□□□
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Astress testevaluates system performance under extreme conditions, such as high user loads, to determine how the system behaves under peak traffic or resource exhaustion.
* Stress Testing (Correct Answer - A)
* Identifies performance bottlenecks in software applications.
* Helps ensure the ERP system can handle expected workloads.
* Example:Simulating thousands of concurrent users accessing the ERP system to test response times and server load capacity.
* Parallel Testing (Incorrect - B)
* Compares a new system with an old one but does not test system performance under load.
* Regression Testing (Incorrect - C)
* Tests whether recent code changes have affected existing functionality but does not focus on performance.
* Interface Testing (Incorrect - D)
* Checks interactions between system components but does not measure performance.
References:
* ISACA CISA Review Manual
* COBIT 2019: Performance and Capacity Planning
* NIST 800-37 (Risk Management Framework)

NEW QUESTION: 457
□□□ □□□□ □□□ □ □□ □□ □□□ □□□□ □□□□ □□ □□ □□□□ □□ □□ □ □□□□□?
A. □□ □□□□ □□□ □□□□ □□ □□
B. □ □□□□ □□ □□ □□ □□
C. □□ □□(QA) □□ □□
D. □□□ □□□□ □□ □ □□ □□□ □□
Answer: (SHOW ANSWER)

The most assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system can be obtained by running historical transactions through the new system.
Historical transactions are transactions that have been processed and recorded by the old system in the past.
Running historical transactions through the new system can provide the most assurance over the completeness and accuracy of loan application processing, by comparing the results and outputs of the new system with those of the old system, and verifying whether they match or differ. This can help identify and resolve any errors or issues that may arise from the new system, such as data conversion, functionality, compatibility, etc.
Comparing code between old and new systems is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Code is a set of instructions or commands that define how a system operates or functions. Comparing code between old and new systems can provide some assurance over the completeness and accuracy of loan application processing, by checking whether the logic, algorithms, or functions of the new system are consistent or equivalent with those of the old system. However, this may not be sufficient or reliable, as code may not reflect the actual performance or outcomes of the system, and may not detect any errors or issues that may occur at the data or user level. Reviewing quality assurance (QA) procedures is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. QA procedures are steps or activities that ensure that a system meets its quality standards and requirements, such as testing, verification, validation, etc. Reviewing QA procedures can provide some assurance over the completeness and accuracy of loan application processing, by evaluating whether the new system has been properly tested and verified before implementation. However, this may not be adequate or accurate, as QA procedures may not cover all aspects or scenarios of loan application processing, and may not reveal any errors or issues that may arise after implementation. Loading balance and transaction data to the new system is a possible way to obtain some assurance over the completeness and accuracy of loan application processing with respect to the implementation of a new system, but it is not the most effective one. Balance and transaction data are data that reflect the status and history of loan applications in a system, such as amounts, dates, payments, etc. Loading balance and transaction data to the new system can provide some assurance over the completeness and accuracy of loan application processing, by transferring data from the old system to the new system and ensuring that they are consistent and correct. However, this may not be enough or valid, as balance and transaction data may not represent all aspects or features of loan application processing, and may not indicate any errors or issues that may arise

NEW QUESTION: 458

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

A. □□ □□□ □□□□□□.

B. □□□ □□□□□□ □□□□□.

C. □□ □□□□ □□□□□□□.

D. □□ □□□ □□ □□□ □□□ □□□□□.

Answer: B (LEAVE A REPLY)

The best recommendation for the IS auditor to make is to implement a closing checklist, as this will help to ensure that all the required tasks and scripts are performed and verified during the year-end closing process12. A closing checklist can also help to prevent errors, omissions, and delays that could affect the accuracy and timeliness of the financial statements3 .

References

1: Year-end closing procedures for GL - Dynamics GP | Microsoft Learn1 2: Year-end activities FAQ - Finance | Dynamics 365 | Microsoft Learn2 3: Year-End Closing Checklist: 10 Steps to Close Your Books3 :

Year End Closing Checklist: 7 Steps to Make it Easy

NEW QUESTION: 459

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

A. □□ □□

B. □□□ □□

C. □□ □□

D. □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 460

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

A. □□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

B. □□ □□□ □□□□ □□ DLP □□□□□□ □□□□ □□□ □□□□□.

C. □□□ □□ □□□□ □□□□ □□ □□□□ □□□□□.

D. □□ □□□ □□ USB □□□ □□□□ □□□ □□□□□.

Answer: D (LEAVE A REPLY)

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: 461
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: 462
□□ □ □□□ □□ □□□□□□ □□ □□□ □□□ □□□□□?

A. □□□□ □□□ □□□ □□
B. □□□□ □□□ □□ □□
C. □□□ □□□□ □□ □□
D. □□□□ □□ □□□ □□□ □□
Answer: C (LEAVE A REPLY)
Determining accountability of data owners is the most important activity in the data classification process.
Data classification is a process that assigns categories or labels to data based on their value, sensitivity, criticality and risk to the organization. Data classification helps to determine the appropriate level of protection, access and retention for data. Determining accountability of data owners is an activity that identifies and assigns roles and responsibilities for data classification, protection and management to individuals or functions within the organization. Data owners are individuals or functions who have authority and responsibility for defining, classifying, protecting and managing data throughout their lifecycle.
Determining accountability of data owners is essential for ensuring that data are classified correctly and consistently, and that data classification policies and procedures are followed and enforced. The other options are not as important as option C, as they are dependent on or derived from the accountability of data owners.
Labeling the data appropriately is an activity that applies the categories or labels assigned by data owners to data based on their classification criteria. Identifying risk associated with the data is an activity that assesses the potential impact and likelihood of loss, disclosure, modification or destruction of data based on their classification level. Determining the adequacy of privacy controls is an activity that evaluates whether the controls implemented to protect personal or sensitive data are sufficient and effective based on their classification level. References: CISA Review Manual (Digital Version) , Chapter 5: Protection of Information Assets, Section 5.3: Data Classification.

NEW QUESTION: 463
□□ □ □□□□ □□ □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□?
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: 464
□□ □□ □□□□ □ □□□ □□ □□(DLP) □□□ □□□□ □□□□ □□ □□ □□ □ □□ □□□□□?
A. □□□ □□□ □□□□ □□ □□□□ □□□□□.
B. □□□ □□□□ □□□ □□□ □□□ □□□□□□.
C. □□□ □□□□ □□□ □□ □□ □□□ □□ □□□□ □□□ □□□□.
D. □□ □□□ SSO(Single Sign-On)□ □□ □□□□ □□□□□□□ □□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 465
□ □□□□ □□□ □□□□□□ □□□□ □□□ □□□ □□ □□□ □ □□ □□ □ □ □□ □□□□□?
A. □□□ □□□
B. □□□ □□□
C. □□□ □□□
D. □□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 466
□□□ □□ □□(DLP) □□□ □□ □□□□ □□□□ □□□ □□□□ □□ □□□ □□ □□□. IS □□□□ □□ □ □□ □□ □□ □□□□ □□□□ □□□?
A. □□□□ □□□□ □□ IT □□□□ □□□□ □□□ □□
B. □□□ □□ □□□ □□ □□□ □□
C. □□ □□□□ □□ □□□□□ □□ □□□ □□
D. IT □□□ □ □□□□□□□ □□ □□□□ □ □□ □□
Answer: C (LEAVE A REPLY)
The associated risk of mobile computing that an IS auditor should identify during the planning phase of a data loss prevention (DLP) audit is increased vulnerability due to anytime, anywhere accessibility. Mobile computing refers to the use of portable devices,

such as laptops, tablets, smartphones, or wearable devices, that can access data and applications over wireless networks from any location6. Mobile computing enables greater flexibility, productivity, and convenience for users, but also poses significant security challenges for organizations. One of these challenges is increased vulnerability due to anytime, anywhere accessibility. This means that mobile devices are exposed to a higher risk of loss, theft, damage, or unauthorized access than stationary devices7. If mobile devices contain or access sensitive data without proper protection, such as encryption or authentication, they could result in data leakage or breach in case of compromise8. Therefore, an IS auditor should identify this risk as part of a DLP audit. The other options are less relevant or incorrect because:

* A. The use of cloud negatively impacting IT availability is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more related to cloud computing than mobile computing. Cloud computing refers to the delivery of computing services, such as data storage or processing, over the Internet from remote servers. Cloud computing may enable or support mobile computing by providing access to data and applications from any device or location, but it does not necessarily imply mobile computing. The use of cloud may negatively impact IT availability if there are disruptions or outages in the cloud service provider's network or infrastructure, but this is not a direct consequence of mobile computing.
* B. Increased need for user awareness training is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a control or mitigation measure than a risk. User awareness training refers to educating users about security policies, procedures, and best practices for using mobile devices and protecting data. User awareness training may help to reduce the risk of data loss or breach due to mobile computing by increasing user knowledge and responsibility, but it does not eliminate or prevent the risk.
* D. Lack of governance and oversight for IT infrastructure and applications is not an associated risk of mobile computing that an IS auditor should identify during the planning phase of a DLP audit, as it is more of a general or organizational risk than a specific or technical risk. Governance and oversight refer to the establishment and implementation of policies, standards, and procedures for managing IT resources and aligning them with business objectives. Lack of governance and oversight for IT infrastructure and applications may affect the security and performance of mobile devices and data, but it is not a direct or inherent result of mobile computing. References: Mobile Computing - ISACA, Mobile Computing Device Threats, Vulnerabilities and Risk Factors Are Ubiquitous - ISACA, Data Loss Prevention-Next Steps - ISACA, [Cloud Computing - ISACA], [Cloud Computing Risk Assessment - ISACA], [User Awareness Training - ISACA], [Governance and Oversight - ISACA]

NEW QUESTION: 467
□□ □ □□□ □□ □□□ 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: 468
IS □□□□ □□ □□□□ □□□ □□□□ □□□ □□(BCP)□ □□□ □□ □□ □□ (RPO)□ □□ □□□□ □□□□ □□ □□□□□□. □□□□ □□□ □□□ □□ □□ □?
A. □□ □□□ □□□□□.
B. □□□□ □□ □□□ □□□□□.
C. □□□□ □□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 469
□□ □ □□ IT□ □□ □□□□□?
A. IT □□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□
B. □□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□
C. IT □□ □□ □□ □□□□ □□□□ □□□ □□□□ □□
D. □□□□ □ □□□□ □□□ □□□□ □□□ □□□□□□ □□□□ □□
Answer: A (LEAVE A REPLY)
Shadow IT refers to the use of IT systems, devices, software, or services without explicit organizational approval. This often occurs when employees or departments adopt tools that bypass official IT governance structures.
* Using a Cloud-Based Order Management Tool Without Approval (Option A)is a clear example of shadow IT because the employee is circumventing established IT policies to implement a solution independently.
* Accessing Personal Banking Information on a Company-Provided Laptop (Option B)is a potential misuse of resources but does not qualify as shadow IT since it does not involve unauthorized technology.
* Using Personal Email for Client Communication (Option C)may violate communication policies but is not related to the adoption of unapproved IT systems.
* Accessing Social Media on a Company-Provided Tablet (Option D)is improper use of a company asset but does not involve unauthorized IT tools.

Shadow IT introduces risks such as data breaches, lack of compliance, and inefficiencies due to lack of integration with official systems. Organizations should have clear policies and monitoring mechanisms to address such risks.
Reference:ISACA CISA Review Manual, Job Practice Area 1: Governance and Management of IT.

NEW QUESTION: 470
□□ □ IT□ □□□□ □□ □□ □□□ □□ IT □□□□□□ □□□□□□ □□ □□□□ □ □□□ □ □□ □□□ □□□□□?
A. □□□□ □□ □□ □□(BIA)
B. □□□□ IT □□ □□ □□
C. □□□□ □□ □□
D. □□□□ IT □□□□□ □□
Answer: D (LEAVE A REPLY)
An IT framework for alignment between IT and business objectives is a set of principles, guidelines, and practices that help an organization to ensure that its IT investments support its strategic goals, deliver value, manage risks, and optimize resources. One of the benefits of implementing such a framework is that it enables an effective IT portfolio management, which is the process of selecting, prioritizing, monitoring, and evaluating the IT projects and services that comprise the IT portfolio. An IT portfolio is a collection of IT assets, such as applications, infrastructure, data, and capabilities, that are aligned with the business needs and objectives. An IT portfolio management helps an organization to achieve the following outcomes:
* Align the IT portfolio with the business strategy and vision
* Balance the IT portfolio among different types of investments, such as innovation, growth, maintenance, and compliance
* Optimize the IT portfolio performance, value, and risk
* Enhance the IT portfolio decision-making and governance
* Improve the IT portfolio communication and transparency
Therefore, an inadequate IT portfolio management is a major concern that can be addressed by implementing an IT framework for alignment between IT and business objectives. An inadequate IT portfolio management can result in the following issues:
* Misalignment of the IT portfolio with the business needs and expectations
* Imbalance of the IT portfolio among competing demands and priorities
* Suboptimal use of the IT resources and capabilities
* Lack of visibility and accountability of the IT portfolio outcomes and impacts
* Poor communication and collaboration among the IT portfolio stakeholders The other possible options are:
* Inaccurate business impact analysis (BIA): A BIA is a process of identifying and assessing the potential effects of a disruption or disaster on the critical business functions and processes. A BIA helps an organization to determine the recovery priorities,

objectives, and strategies for its business continuity plan. A BIA is not directly related to an IT framework for alignment between IT and business objectives, although it may use some inputs from the IT portfolio management. Therefore, an inaccurate BIA is not a concern that can be effectively addressed by implementing an IT framework for alignment between IT and business objectives.
* Inadequate IT change management practices: IT change management is a process of controlling and managing the changes to the IT environment, such as hardware, software, configuration, or documentation. IT change management helps an organization to minimize the risks and disruptions caused by the changes, ensure the quality and consistency of the changes, and align the changes with the business requirements. IT change management is not directly related to an IT framework for alignment between IT and business objectives, although it may support some aspects of the IT portfolio management. Therefore, inadequate IT change management practices are not a concern that can be effectively addressed by implementing an IT framework for alignment between IT and business objectives.
* Lack of a benchmark analysis: A benchmark analysis is a process of comparing an organization's performance, processes, or practices with those of other organizations or industry standards. A benchmark analysis helps an organization to identify its strengths and weaknesses, set realistic goals and targets, and implement best practices for improvement. A benchmark analysis is not directly related to an IT framework for alignment between IT and business objectives, although it may provide some insights for the IT portfolio management. Therefore, lack of a benchmark analysis is not a concern that can be effectively addressed by implementing an IT framework for alignment between IT and business objectives. References: 1: What is Portfolio Management? | Smartsheet 2: What Is Portfolio Management? - Definition from Techopedia 3: What Is Project Portfolio Management (PPM)? | ProjectManager.com 4: What Is Business Impact Analysis? | Smartsheet 5: What Is Change Management? - Definition from Techopedia 6: Benchmarking - Wikipedia

NEW QUESTION: 471
□□ □□□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□ □□□ □□, IS □□□ □ □□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□□ □□ □□□ □□□ □□□□□ □□□.
B. □□□ □□□ □□□□ □□ □□ □□□ □□□□□.
C. □□□ □□□ □□ □□ □□□ □□□□□.
D. □□□ □□□ □□ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit is to evaluate the residual risk due to open issues. Residual risk is the risk that remains after the implementation of controls or mitigating actions. Evaluating the residual risk due to open issues can help the IS auditor

assess the impact and likelihood of the potential threats and vulnerabilities that have not been addressed by the auditee, as well as the adequacy and effectiveness of the existing controls or mitigating actions. Evaluating the residual risk due to open issues can also help the IS auditor prioritize and communicate the open issues to the auditee and other stakeholders, such as senior management or audit committee, and recommend appropriate actions or escalation procedures.
Ensuring the open issues are retained in the audit results is a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but it is not the best one. Ensuring the open issues are retained in the audit results can help the IS auditor document and report the status and progress of the audit recommendations, as well as provide a basis for future follow-up audits.
However, ensuring the open issues are retained in the audit results does not provide an analysis or evaluation of the residual risk due to open issues, which is more important for informing decision-making and action- taking.
Terminating the follow-up because open issues are not resolved is not a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but rather a consequence or outcome of it. Terminating the follow-up because open issues are not resolved may indicate that the auditee has failed to comply with the agreed-upon actions or deadlines, or that the IS auditor has encountered significant obstacles or resistance from the auditee. Terminating the follow-up because open issues are not resolved may also trigger further actions or sanctions from the IS auditor or other authorities, such as issuing a qualified or adverse opinion, withholding certification, or imposing penalties.
Recommending compensating controls for open issues is not a course of action for an IS auditor when an auditee is unable to close all audit recommendations by the time of the follow-up audit, but rather a possible outcome or result of it. Compensating controls are alternative or additional controls that are implemented to reduce or eliminate the risk associated with a weakness or deficiency in another control. Recommending compensating controls for open issues may be appropriate when the auditee is unable to implement the original audit recommendations due to technical, operational, financial, or other constraints, and when the compensating controls can provide a similar or equivalent level of assurance. However, recommending compensating controls for open issues requires a prior evaluation of the residual risk due to open issues, which is more important for determining whether compensating controls are necessary and feasible.
References:
* Follow-up Audits - Canadian Audit and Accountability Foundation 1
* Conducting The Audit Follow-Up: When To Verify - The Auditor 2
* Internal Audit Follow Ups: Are They Really Worth The Effort

NEW QUESTION: 472

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

A. □□ □□□□ □□

B. ISP □□□ □□ □□

C. □□□□ □□□ □□ □□□

D. □□□□ □□□□ □□□□□

Answer: (SHOW ANSWER)

Network topology diagrams are the most important for an IS auditor to review when evaluating the design of controls related to network monitoring, because they show how the network components are connected and configured, and what security measures are in place to protect the network from unauthorized access or attacks. Incident monitoring logs, the ISP service level agreement, and reports of network traffic analysis are useful for evaluating the effectiveness and performance of network monitoring, but not the design of controls. References: CISA Review Manual (Digital Version), Chapter 5, Section 5.3.3

NEW QUESTION: 473

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

A. □□ □□□□□

B. □□□□□□ □□ □□□□□

C. □□ □□□ □□□

D. □□□□ □□□

Answer: B (LEAVE A REPLY)

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: 474
IS □□□□ □□ □□ □□□ □□□□ □□□ □□□□□□ □□□□ □□ □□□ □□ □□ □□ □□□ □□ □□□ □□□□ □□□□. □□□□ □ □□□ □□□□ □□ □□ □□ □□ □□□□?
A. □□□ □□□ □□ □□ □□□
B. □□□□□□ □□
C. □□ □□
D. □□ □□ □ □□□ □□(SIEM) □□□
Answer: C (LEAVE A REPLY)
A change log is a record of all changes made to a system or application, including the date, time, description, and approval of each change. A change log can help an IS auditor to trace the source and authorization of a modification to a system's security settings. A system event correlation report is a tool that analyzes data from multiple sources to identify patterns and anomalies that indicate potential security incidents. A database log is a record of all transactions and activities performed on a database, such as queries, updates, and backups. A security incident and event management (SIEM) report is a tool that collects, analyzes, and reports on data from various sources to detect and respond to security incidents.

NEW QUESTION: 475
□□□□ □□□ □□□ □ □□ □□□ □□ □□□□□?
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: 476
□□ □□ □□□□ □ □□ □□□ □□□ □□□□.
A. □□□ □□ □□□ □□□ □□ □□□□□.
B. □□□ □□□□ □□□ □ □□ □□ □□□□ □□ □□□ □ □□□□.
C. □□□ □□ □□ □□□ □□□□ □□□ □□□□□.
D. □□□□ □□ □□□□ □□□ □□□□ □□□□.
Answer: (SHOW ANSWER)
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: 477
□□□ □□ □□□ □□□ □□□□□□□ □□□□ □□ □□□ □□□□ □□□□□ □ □ □□□ □□□□□□ □□□□ □□ □□ □ □□ □□□ □□□ □□□?
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: 478
□□ □ □□ □□□ □□□ □□□ □□□□ □□□ □□□□□□□ □□□ □□□□ □□ BE ST □□□ □□□□ □□ □□□□□?
A. □□ □□□ □□ □□ □□□
B. □□□ □□ □□(MDM) □□
C. □□□□ □□□□ □□ □□ □□□□
D. □□□ □□□□ □□ □□ □□ □□ □□
Answer: B (LEAVE A REPLY)
The best method for maintaining the security of corporate applications pushed to employee-owned mobile devices is implementing mobile device management (MDM). MDM is a software solution that allows an organization to remotely manage, configure, and secure the mobile devices that access its network and data.
MDM can help protect corporate applications on employee-owned devices by:
Enforcing security policies and settings, such as encryption, password, firewall, antivirus, and VPN.
Controlling the installation, update, and removal of corporate applications and data.
Separating corporate and personal data and applications on the device using containers or profiles.
Monitoring and auditing the device's compliance status, activity, and location.
Performing remote actions, such as lock, wipe, backup, or restore, in case of loss, theft, or compromise.

MDM can provide a comprehensive and centralized approach to maintain the security of corporate applications on employee-owned devices, regardless of the device type, platform, or ownership. MDM can also help the organization comply with regulatory and industry standards for data protection and privacy.
Enabling remote data destruction capabilities is a useful feature for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Remote data destruction allows the organization to erase the corporate data and applications from the device in case of loss, theft, or compromise. However, this feature does not prevent unauthorized access or misuse of the corporate data and applications before they are destroyed. Remote data destruction is usually part of an MDM solution.
Disabling unnecessary network connectivity options is a good practice for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Network connectivity options, such as Wi-Fi, Bluetooth, NFC, or USB, can expose the device to potential attacks or data leakage. Disabling these options when they are not needed can reduce the attack surface and improve battery life. However, this practice does not address other security risks or requirements for the corporate applications on the device. Disabling network connectivity options can also be part of an MDM solution.
Requiring security awareness training for mobile users is an important measure for maintaining the security of corporate applications on employee-owned devices, but it is not the best method by itself. Security awareness training can educate the users about the potential threats and best practices for using their devices securely. It can also help foster a culture of security and responsibility among the users. However, security awareness training cannot guarantee that the users will follow the security policies and guidelines consistently and correctly. Security awareness training should be complemented by technical controls, such as MDM.
References:
Protecting Corporate Data on Mobile Devices for All Companies1
Mobile Device Security: Corporate-Owned Personally-Enabled (COPE)23

NEW QUESTION: 479
□□□□ □□□ □□□ □□ □□(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: 480
□□ □□□□□ □□□ □□□ □□□□□ □ □□□ □□□□ □□□. □□□ □ □□□ □□ □□ □□□ □□□ □□□ □□□□□□□. □□ □□□ □□□ □□□□□□□?
A. □□
B. □□
C. □□
D. □□□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 481
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: 482
□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□□□.
□□ □ 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: 483
□□□□□ □□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□ IS □□□□ □□ □□ □□□?
A. □□□ □ □□
B. □□ □□ □□□
C. □□□□□ □□
D. □□□□ □□

Answer: D (LEAVE A REPLY)
An IS auditor should be consulted during the requirements definition phase to recommend security controls.
This ensures that security considerations are integrated from the beginning of the software development life cycle, leading to more secure software design and implementation.
References
* ISACA CISA Review Manual 27th Edition, Page 240-241 (SDLC Phases)

NEW QUESTION: 484
□□ □ □□ □ □□ IT□ □□ □□□□ □□ □□□ □□ □□ □□□□□?
A. □□ □□□ □□ □□ □□
B. □□□□□ □□□□ □□□ □□ □ □□ □□
C. □□□□ □□ □□□□□□ □ □□□□ □□ □□□
D. □□□ □□□□□□ □□□ □□ □□□ □□□□ □□
Answer: (SHOW ANSWER)
Shadow IT often arises whenapproved software does not meet user requirements(Option D), leading employees to seek alternative solutions.
ISACA CISA Reference:IT governance frameworks stress the need for user-centric IT policies to mitigate shadow IT risks.
Risk Implication:Shadow IT introduces security vulnerabilities, compliance risks, and potential data breaches.

NEW QUESTION: 485
IT □□□□ □□□□□□ □□□□□ □□□ □□□□ □□□ □□□□ □□□.
A. □□□□ IT □□□ □□□□□.
B. □□ IT □□□□□□ □□ □□□□□.
C. IT □□ □□□□ □□□□□.
D. IT □□□ □□□□□.
Answer: D (LEAVE A REPLY)
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: 486
□□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □ □□ □□□□ □□ □□ □□□ □□□□□ □□□ □□□□□□. □□ □ □□ □□□ □□ □□□ □□□ □□ □ □□□□□?
A. □□□□□□□ □□□ □□□□ □□□□□ □□□□ □□□ □

B. □□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□ □□□ □□□ □
C. □□□ □□□□□ □□□□ □□□□ □□□ □
D. □□□□□□ □□□ □□□ □□□ □□□ □
Answer: D (LEAVE A REPLY)
The metric that best indicates the effectiveness of awareness training is the number of users reporting receipt of the email to the information security team. This shows that the users are able to recognize and report a phishing email, which is a common social engineering technique used by attackers to trick users into revealing sensitive information or installing malicious software. The other metrics do not demonstrate a high level of security awareness, as they either ignore, follow, or forward the phishing email, which could expose the organization to potential risks. References: CISA Review Manual, 27th Edition, page 326

NEW QUESTION: 487
□□ □□ □□ □□ □□ □ BE ST□ BYOD(Bring Your Own Device) □□□□ □□ □□ □□ □□□ □ □□ □□ □□ □□□□□?
A. □□□ □□ □□□□ □□□ □□□ □□□ □□ □□ □□□□ □□ □□ □□□□ □ □□.
B. □□□ □□□ □□□ □□ □□ □□ □□□ □□ □□□□ □□□□ □□□.
C. □□□ □□□ □□□ □□ □□ □□□□□ □□ □□□ □□□□ □□□.
Answer: (SHOW ANSWER)
The best way to track organizational data in a BYOD environment is to enroll the personal devices in the organization's mobile device management (MDM) program. This will allow the organization to monitor, control, and secure the data on the devices remotely. Employees must also report lost or stolen devices and sign the acceptable use policy, but these are not sufficient to enable tracking of data. References: Info Technology & Systems Resources |COBIT, Risk, Governance ... - ISACA, section "Book IT Control Objectives for Sarbanes-Oxley, 4th Edition | Digital | English"

NEW QUESTION: 488
IS □□□□ □□□□ □□ □□□□ □□□ □□□ □□□□ □□□□. □□□ □□□□ □ □□□ □□□ □□□□□ □□□□ □□□□ □□□□ □□ □□ □□□ □□ □ □□ □□□□?
A. □□ □□□ □□
B. □□ □□ □□
C. □□□ □□ □
D. □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 489

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

A. □□□□□ □□ □□ □□

B. □□□□ □□□□□ □□□□

C. □□□ □□□□□ □□ □□□ □□ □□

D. □□ □□ □□ □□ □□

Answer: (SHOW ANSWER)

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: 490

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

A. □□□□ □□ □□□□ □□.

B. □□ □□□□□ □□□□ □□ □□□□□□□.

C. □□□ □□□ □□□ □□□ □□□□□□ □□.

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

Answer: C (LEAVE A REPLY)

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: 491

□□□ □□□□ □□□ □□□□□ □□ □□□□ □□□ □□□ □ 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: 492
□3□ □□□□□ □□ □□□ □□□ □□□□ □□□□. □□ □ IS □□□□ □□ □ □ □□□ □□□□□?
A. □□□ □□□□□□□ □□□ □□□ □□□□ □□□□.
B. □□□ □□ □□□ □□□□□ □□□□.
C. □□□ □□□ □□ □□□ □□□□□.
D. □□□□ □3□ □□□□□ □□ □□□□□□□.
Answer: C (LEAVE A REPLY)
The greatest concern for an IS auditor in this scenario is that the user department will manage access rights to the new accounting system. This could pose a significant risk of unauthorized access, segregation of duties violations, data tampering and fraud. The IS auditor should ensure that access rights are defined, approved and monitored by an independent function, such as IT security or internal audit. The other options are not as concerning as option C, as they can be mitigated by other controls or procedures. Data migration is an important part of the system replacement project, but it can be performed by another party or verified by the IS auditor. The timing of the replacement near year-end reporting is a challenge, but it can be managed by proper planning, testing and contingency plans. Testing performed by the third-party consultant is acceptable, as long as it is reviewed and validated by the IS auditor or another independent party. References: CISA Review Manual (Digital Version) 1, Chapter 3: Information Systems Acquisition, Development & Implementation, Section 3.4: System Implementation.

NEW QUESTION: 493
□□ □□□□ □□ □□ □□□□ □□□ □□ □□ □□ □□□ □□□□ □□□□.
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: 494
□□□□ □□ □□□□□□ □□□□□ □□□□□ □□□□□ □□ □□□□ □□□ □ □□ □□□?
A. □□ □□ □□□ □□□□ □□ □□□□□ □□□.
B. □□□□ □□□□□(DMZ)□ □□□□ □□□.
C. □□ □□□ □□ □□□ □□□□ □□□.
D. □□□□ □□ □□□□ □□□□□ □□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 495
□□ □ □□□ □□□□□ □□□ □ □□ □□ □□□□□?
A. □□□□
B. 256-brt □ □□
C. □□□ □□□
D. □□ □□
Answer: D (LEAVE A REPLY)
The only thing that can be provided by asymmetric encryption is nonrepudiation. Nonrepudiation is the ability to prove that a message or transaction was originated or authorized by a specific party. Asymmetric encryption uses a pair of keys: a public key and a private key. The public key can be shared with anyone, while the private key is kept secret by the owner. If a message is encrypted with the sender's private key, only the sender's public key can decrypt it. This proves that the message was sent by the sender and not by anyone else. This is called digital signature and it provides nonrepudiation. Asymmetric encryption can also provide information privacy by encrypting a message with

the receiver's public key, so that only the receiver's private key can decrypt it. However, information privacy can also be provided by symmetric encryption, which uses a single key to encrypt and decrypt messages. References:
* CISA Review Manual (Digital Version), Chapter 5, Section 5.21
* CISA Online Review Course, Domain 3, Module 2, Lesson 12

NEW QUESTION: 496
□□ □□□□ □□ □□□ □□□□ □□□□ □□□□ □□□□ □□□□□ □□ □□□ □□□□ □□ □□□□ □□□ □□ □ □□□□□?
A. □□□□ □□□□□ □□□ □□□ □□ □□
B. □□□□ □□□□□ □□□ □□□ □□□□ □□□□ □□
C. □□□□ □□□□□ □□ □□□□□ □□□ □□□□ □□□□ □□□□□.
D. □□ □□□ □□ □□□ □□ □□ □□
Answer: (SHOW ANSWER)
Reviewing the last compile date of production programs is the most efficient way to detect unauthorized changes to production programs, as it can quickly identify any discrepancies between the expected and actual dates of program modification. The last compile date is a timestamp that indicates when a program was last compiled or translated from source code to executable code. Any changes to the source code would require a recompilation, which would update the last compile date. The IS auditor can compare the last compile date of production programs with the authorizedchange requests and reports to verify that only approved changes were implemented. The other options are not as efficient as option A, as they are more time-consuming, labor- intensive or error-prone. Manually comparing code in production programs to controlled copies is a method of verifying that the code in production matches the code in a secure repository or library, but it requires access to both versions of code and a tool or technique to compare them line by line. Periodically running and reviewing test data against production programs is a method of verifying that the programs produce the expected outputs and results, but it requires designing, executing and evaluating test cases for each program.
Verifying user management approval of modifications is a method of verifying that the changes to production programs were authorized and documented, but it does not ensure that the changes were implemented correctly or accurately. References: CISA Review Manual (Digital Version) , Chapter 4: Information Systems Operations and Business Resilience, Section 4.3: Change Management Practices.

NEW QUESTION: 497
□□□ □□□□ □□ □□□ □□□□□ □□□ □□□□ □□□ □□ □□□□ □□□□.
IS □□□□ □□□ □□□□ □□□ □□□ □□□□ □ □□ □□□ □□ □□ □□ □ □ □ □□□□?
A. □□□ □□ □□ □□(CAAT)
B. □□□ □□□
C. □□□ □□□
D. □□□□ □□
Answer: A (LEAVE A REPLY)
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: 498
□□ □ □□□ □□ □□□□□□ □□□ □□ □□ □ □□ □□ □□ □□□□ □□□□ □?
A. □□□□□□□(IPS)
B. □□□□ □□ □□
C. □□ □□ □□
D. □□ □□ □□□(IDS)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 499
□□□□□ □□ □□□ □□□ □□□□□□ □□□□ □□ □□, □□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□□.
A. □□□ □□□□ □ □□□ □□□ □ □□□ □□□□□ □□□□□□□.
B. □□□□ □□□ □□□□ □□ □□□ □□□□□.

C. □□□□ □□□ □□□□ □□ □□□□ □□□□□□□.
D. □□□□ □□□□ □□ □□□ □ □□ □□□□□.
Answer: C (LEAVE A REPLY)
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: 500
□□ □ □□□ IT □□□ □□□□□□ □□□□(EA) □□ □ □□ □□□ □□□□□ □□ □□ □□ □□ □□□ □□□□□?
A. EA□ □□□ □□ □□ □□□□□□.
B. EA□ □□□ □ □□ □□□□ □□ □□□ □□□□□.
C. IT □□□ □□ □□ □□ □□ □□ □□
D. □□ □□ □□□□ □□□ EA □□ □□
Answer: (SHOW ANSWER)
The best way to help ensure new IT implementations align with enterprise architecture (EA) principles and requirements is to conduct EA reviews as part of the change advisory board (CAB). A CAB is a committee that evaluates and authorizes changes to IT services, such as new IT implementations. By conducting EA reviews as part of the CAB process, the organization can ensure that the proposed changes are consistent with the EA vision, goals, standards, and guidelines. This can help avoid potential conflicts, risks, or inefficiencies that may arise from misaligned IT implementations. Additionally, EA reviews can help identify opportunities for improvement, optimization, or innovation in the IT services.
The other options are not the best ways to help ensure new IT implementations align with EA principles and requirements. Documenting the security view as part of the EA is important, but it does not guarantee that new IT implementations will follow the security requirements or best practices. Considering stakeholder concerns when defining the EA is also essential, but it does not ensure that new IT implementations will meet the stakeholder expectations or needs. Performing mandatory post-implementation reviews of IT implementations is a good practice, but it does not prevent potential issues or problems that may arise from misaligned IT implementations.
References:
* 5: Change Advisory Board Best Practices: 15+ Industry Leaders Weigh In
* 6: What Does the Change Advisory Board (CAB) Do?
* 7: How do I set up an effective change advisory board? - ServiceNow
* 8: ITIL Change Management - The Role of the Change Advisory Board

NEW QUESTION: 501
□□□□□□ □□ □□□(DBMS)□ □□□ □□ □□□ □□□ □□ □□□ □□□.
A. □□□□ □□ □□□□ □□□ □□□□□.
B. □□□□□□ □□□(DBA)□ □□□ □□□ □□□ □ □□□ □□□.
C. □□□□ □□□ □□□ □□ □□ □□□□ □□ □□□□□.
D. □□□□ □□ □□□ □□□ □□□ □□□□ □□□ □□ □ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The record-locking option of a database management system (DBMS) serves to eliminate the risk of concurrent updates to a record by different users or transactions. Record locking is a technique of preventing simultaneous access to data in a database, to prevent inconsistent results1. For example, if two bank clerks try to update the same bank account for two different transactions, record locking can ensure that only one clerk can modify the record at a time, while the other has to wait until the lock is released. This way, the record will reflect both transactions correctly and avoid data corruption.
Record locking does not serve to allow database administrators (DBAs) to record the activities of users. This is a function of auditing or logging, which can track the actions performed by users on the database2. Record locking does not affect the ability of DBAs to monitor or audit user activities.
Record locking does not serve to restrict users from changing certain values within records. This is a function of access control or authorization, which can enforce rules or policies on what data users can view or modify2. Record locking does not affect the permissions or privileges of users on the database.
Record locking does not serve to allow users to lock others out of their files. This is a function of encryption or password protection, which can secure files from unauthorized access or modification3. Record locking does not affect the security or confidentiality of files on the database.
References:
Record locking - Wikipedia1
Database security - Wikipedia2
File system permissions - Wikipedia3

NEW QUESTION: 502
□□ □ IS □□ □□□□ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□□ □□ □□□ □□□□ □□ □□□
B. □ □□ □□□ □□ □□ □□ □□□
C. □□□□ □□□ □□ □□□□ □□ □□ □□
D. □□□ □□□□ □□□□□□ □□□□ □□ □□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 503

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

A. □□ □□□ □□□□ □□□ □□□, □□□□□, □□□□ □□ □□□ □□□□□.

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

C. □□□ ID□ □□□□ □□□□ □□□□ □□□ □□□ □□□□ □□□□□.

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

Answer: (SHOW ANSWER)

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: 504

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

A. □□□ □□

B. □□□□ □□ □□□

C. □□□□

D. □□ □□□□

Answer: C (LEAVE A REPLY)

When a data center is attempting to restore computing facilities at an alternative site following a disaster, the operating system should be restored FIRST. Here's why:

1. Operating System (OS):

The OS is the foundation of any computing environment. It manages hardware resources, provides essential services, and allows applications to run.

Restoring the OS ensures that the infrastructure is operational and ready for further recovery steps.

Without a functional OS, applications cannot execute, and data backups cannot be effectively restored.

2. Data Backups:

While data backups are critical for recovery, they depend on a working infrastructure.

If the OS is not operational, restoring data backups becomes challenging.

Data backups should follow the OS restoration.
3. Applications:
Applications rely on the OS to function.
Restoring applications before the OS may lead to compatibility issues or incomplete functionality.
Applications should be restored after ensuring a stable OS environment.
4. Decision Support System (DSS):
DSS is an application category.
It should follow the restoration of both the OS and critical applications.
In summary, prioritize restoring the operating system, which forms the basis for subsequent recovery steps12.
Once the OS is functional, proceed with data backups, applications, and other systems as needed.

NEW QUESTION: 505
□□ □ □□□ □□□ □□□ □ □□ □□□ □□ □□□□□?
A. □□ □□□□ □□□□ □□ □□
B. □□□□□ □□ □□□ □□□ □□ □□ □□□
C. □□□ □□□ □□□□□ □□ □□□ □□□□□ □□
D. □□□ □□□ □□□ □ □□□□ □□
Answer: A (LEAVE A REPLY)
Computer performance is the measure of how well a computer system can execute tasks and applications within a given time frame. Computer performance can be affected by various factors, such as hardware specifications, software configuration, network conditions, and user behavior. To analyze computer performance, it is important to use statistical metrics that can quantify the capacity utilization of the system resources, such as CPU, memory, disk, and network. These metrics can help identify the bottlenecks, inefficiencies, and anomalies that may degrade the performance of the system. Examples of such metrics include CPU utilization, memory usage, disk throughput, network bandwidth, and response time.
The other options are not as useful as statistical metrics when analyzing computer performance. An operations report of user dissatisfaction with response time is a subjective measure that may not reflect the actual performance of the system. Tuning of system software to optimize resource usage is a corrective action that can improve performance, but it is not a method of analysis. A report of off-peak utilization and response time is a limited snapshot that may not capture the peak performance or the average performance of the system.
References:
* What is Computer Performance?
* How to Measure Computer Performance

NEW QUESTION: 506
□□ □□□ □□□□ □□ □□ □□ □□ □□ □ □□ □□□ □□ □□□□□?
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: 507
□□ □ □□ □□(QA) □□ □□ □□□ □□□□□?
A. □□□ □□ □□□(IJAT) □□□□□ □□□□ □□ □□ □□□ □□□ □□
B. □□ □□□ □□□□ □ □□ □□ □□
C. □□ □□ □□ □ □□ □□□ □□ □□□□□□ □□ □□
D. □□ □□ □□ □□ □□□ □□□□ □□ □□ □□
Answer: D (LEAVE A REPLY)
A quality assurance (QA) team is a group of professionals who are responsible for ensuring that the products or services of an organization meet the quality standards and expectations of customers and stakeholders1. A QA team performs various activities, such as:
Planning, designing, and executing quality tests and audits to verify the quality of the products or services1 Identifying, analyzing, and reporting quality issues, defects, or non-conformities1 Recommending and implementing corrective and preventive actions to resolve quality problems and prevent recurrence1 Monitoring and measuring the effectiveness and efficiency of the quality processes and improvements1 Establishing and maintaining quality documentation, records, and reports1 Providing quality training, guidance, and support to the staff and management1 One of the primary responsibilities of

a QA team is to implement procedures to facilitate adoption of quality management best practices. Quality management best practices are the methods, techniques, or tools that have been proven to be effective in achieving and maintaining high-quality standards in an organization2. Some examples of quality management best practices are:
Adopting a customer-focused approach that aims to meet or exceed customer requirements and satisfaction2 Implementing a process approach that manages the interrelated activities as a coherent system2 Applying continuous improvement methods that seek to enhance the performance and value of the products or services2 Using evidence-based decision making that relies on factual data and information2 Developing a culture of engagement and empowerment that involves and motivates the people in the organization2 By implementing procedures to facilitate adoption of quality management best practices, a QA team can help the organization achieve the following benefits:
Improve the quality and reliability of the products or services2
Reduce the costs and risks associated with poor quality or non-compliance2 Increase the customer loyalty and retention2 Enhance the reputation and competitiveness of the organization2 Foster a culture of excellence and innovation in the organization2 The other options are not primary responsibilities of a QA team. Creating test data to facilitate the user acceptance testing (UAT) process is a task that can be performed by a QA team, but it is not their main duty. UAT is a process in which the end users test the product or service to ensure that it meets their needs and expectations before it is released or deployed3. A QA team can create test data to simulate real-world scenarios and conditions for UAT, but they are not directly involved in conducting UAT. Managing employee onboarding processes and background checks is not a responsibility of a QA team. Employee onboarding is a process in which new hires are integrated into the organization, while background checks are screenings that verify the identity, credentials, and history of potential employees4. These processes are usually handled by the human resources department or an external agency, not by a QA team. Advising the steering committee on quality management issues and remediation efforts is not a primary responsibility of a QA team. A steering committee is a group of senior executives or managers who provide strategic direction, oversight, and support for a project or program5. A QA team can advise the steering committee on quality management issues and remediation efforts, but they are not accountable for making decisions or implementing actions. Therefore, option D is the correct answer.
References:
Quality Assurance Team: Roles & Responsibilities
What are the Best Practices in Quality Management?
User Acceptance Testing (UAT): A Complete Guide
Employee Onboarding Process: Definition & Best Practices
What Is A Steering Committee? - The Basics

NEW QUESTION: 508

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

A. □□□□□□ □□□□(EA)

B. □□ □□ □□(BIA)

C. □□□ □□ □□□

D. □□ □□ □□

Answer: (SHOW ANSWER)

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: 509

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

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

B. □□□ □□□ □□□□ □□□□ □□□□□□□□.
C. □□□ □□□ □□□ □□ □□□□ □□□□□.
D. □□ □□ □ □□□ □□ □□□ □□□ □□□□.
Answer: (SHOW ANSWER)
Clear criteria ensure a consistent, rational approach to risk acceptance decisions, demonstrating management's deliberate and informed approach to risk management.
References
ISACA CISA Review Manual (Current Edition) - Chapter on Risk Management Risk Management Frameworks (e.g., ISO 31000, NIST SP 800-39) - Emphasize the importance of defined risk assessment and decision-making processes.

NEW QUESTION: 510
□□ □ □□ □□□ □□ □□□□□ □□□□□ □□□□ □ □□ □□□ □□ □□□□ □?
A. □□□ □□ □□ □□
B. □□□□ □□ □□□□
C. □□□□ □□ □□ □□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)
A comprehensive asset inventory is the most important factor for the successful establishment of a security vulnerability management program. A security vulnerability management program is a systematic process of identifying, assessing, prioritizing, and remediating vulnerabilities in the organization's IT environment1. A comprehensive asset inventory is a complete and accurate record of all the hardware, software, and network components that the organization owns or uses2. A comprehensive asset inventory helps the organization to:
Know what assets are in scope for vulnerability scanning and assessment3.
Identify the vulnerabilities that affect each asset and their severity level4.
Prioritize the remediation of vulnerabilities based on the criticality and value of each asset.
Track the status and progress of vulnerability remediation for each asset.
Measure the effectiveness and maturity of the vulnerability management program.
A robust tabletop exercise plan is a simulated scenario that tests the organization's preparedness and response capabilities for a potential cyberattack or incident. A tabletop exercise plan is useful for validating and improving the organization's incident response plan, but it is not essential for establishing a security vulnerability management program.
A tested incident response plan is a documented process that defines the roles, responsibilities, and actions of the organization's personnel in the event of a cyberattack or incident. A tested incident response plan is important for minimizing the impact and restoring normal operations after a security breach, but it is not critical for establishing a security vulnerability management program.

An approved patching policy is a set of rules and guidelines that governs how the organization applies patches and updates to its IT systems and applications. An approved patching policy is a key component of the remediation phase of the vulnerability management program, but it is not sufficient for establishing a security vulnerability management program.

NEW QUESTION: 511
□□ □ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□ □□□?
A. □□□ □□ □□
B. □□ □□□ □□□□ □□
C. □□ □ □□ □□
D. □□□□ □□ □□
Answer: (SHOW ANSWER)
Using risk assessments to determine areas to be included in an audit plan is a primary benefit because it helps to prioritize the audit activities based on the level of risk and the potential impact of the audit findings. This way, the audit resources, such as time, staff, and budget, can be allocated more efficiently and effectively to the areas that need the most attention and provide the most value.
References
ISACA CISA Review Manual, 27th Edition, page 256
What is the Purpose of a Risk Assessment?
Mastering the Process of Risk Assessment

NEW QUESTION: 512
IS □□□□ □□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□□ □□ □ □□ □□ □□ □□□ □□□□□□. □□□□ □□ □□□ □□ □ □□ □□□□?
A. □□□ □□□ □□□□□.
B. □□ □□ □□□□□ □□□□□.
C. □□ □□ □□□□□ □□□□□.
D. □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

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: 513
□□ □ □□ □□ □□□□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□ □ □□ □□ □□□ □□□□□?
A. □□□□ □□□ □□□□□□ □□ □□□ □□□□□.
B. □□□□ □□□ □□□ □□□□ □□□□ □□□.
C. □□□□ □□□ □□□□ □□□ □□ □□□ □□□□□□.
D. □□□□ □□□ □□ □□□ □□ □□□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
During a pre-deployment assessment, the best indication that a business case will lead to the achievement of business objectives is that the business case reflects stakeholder requirements. A business case is a document that explains the rationale, benefits, costs, and risks of a proposed project or initiative. A business case should align with the strategic goals and vision of the organization and address the needs and expectations of the stakeholders who are involved in or affected by the project12.
Stakeholder requirements are the conditions or capabilities that stakeholders expect from a project or its outcomes. Stakeholders can include customers, users, employees, managers, suppliers, regulators, and others who have an interest or stake in the project. Stakeholder requirements should be identified, analyzed, prioritized, validated, and documented throughout the project lifecycle34.
The business case should reflect stakeholder requirements because they provide the basis for defining the project scope, objectives, deliverables, quality standards, success criteria, and benefits realization. By reflecting stakeholder requirements, the business case can demonstrate how the project will add value to the organization and its stakeholders, justify the investment and resources required for the project, and facilitate the decision-making and approval process for the project5 .
Therefore, during a pre-deployment assessment, an IS auditor should look for evidence that the business case reflects stakeholder requirements as the best indication that the business case will lead to the achievement of business objectives.

References:
How to Write a Business Case (Template Included) - ProjectManager
How to Write a Business Case | Smartsheet
What are Stakeholder Requirements? | PM Study Circle
Stakeholder Requirements - Project Management Knowledge
Business Case vs Business Requirements - Difference Between
[Business Case Development - Project Management Docs]

NEW QUESTION: 514
□□ □ □□ □□□□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□□?
A. □□□ □□□□ □□□ □□ □□□□ □□□□ □□□ □□ □ □□□ □□
B. □□□□ □□□□□ □□□□ □ □□□ □□□□ □
C. □□□□ □□□□ □□□ □□□ □□□ □□□□ □□□□□□.
D. □□□□□ □□ □□□□□ □□ □□□□□ □□
Answer: B (LEAVE A REPLY)
Requiring a key code to be entered on the printer to produce hard copy is a method to prevent disclosure of classified documents printed on a shared printer. This is because requiring a key code adds an extra layer of security and authentication to the printing process, ensuring that only authorized users can access and retrieve the printed documents. Requiring a key code also prevents unauthorized users from viewingor tampering with the documents while they are in the printer's queue or output tray1.
Using passwords to allow authorized users to send documents to the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because passwords only protect the transmission of the documents from the user's computer to the printer, but they do not protect the documents once they are printed. Passwords can also be compromised or forgotten by users, making them vulnerable to unauthorized access or denial of service2.
Encrypting the data stream between the user's computer and the printer is not a sufficient method to prevent disclosure of classified documents printed on a shared printer. This is because encryption only protects the confidentiality and integrity of the documents while they are in transit, but they do not protect the documents once they are printed. Encryption can also introduce performance issues or compatibility problems with different printers or devices2.
Producing a header page with classification level for printed documents is not a method to prevent disclosure of classified documents printed on a shared printer. This is because producing a header page only informs the users about the sensitivity and handling of the documents, but it does not prevent unauthorized users from accessing or viewing them. Producing a header page can also waste paper and ink, as well asincrease the risk of misplacing or mixing up the documents

NEW QUESTION: 515

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

A. □□ □□□ □□ □□ □□□ □□ □□□□ □□□□□.

B. □□ □□□ □□□ □□□ □□□□ □□□□ □□□□□.

C. □□□□ □□□□□ □□ □□□□ □□□□.

D. □□ □□□□ □□□ □□ □□□□ □□□□ □□□□□.

Answer: B (LEAVE A REPLY)

The audit finding that should be of greatest concern is that tasks defined on the critical path do not have resources allocated, as this means that the project is likely to face significant delays and cost overruns, since the critical path is the sequence of activities that determines the minimum time required to complete the project. The actual start times of some activities being later than originally scheduled may indicate some minor deviations from the project plan, but they may not necessarily affect the overall project completion time if they are not on the critical path. The project manager lacking formal certification may affect the quality and efficiency of the project management process, but it does not necessarily imply that the project manager is incompetent or unqualified. Milestones have been defined for all project products, but they may not be realistic or achievable if they do not take into account the resource constraints and dependencies of the critical path tasks. References: CISA Review Manual (Digital Version), Chapter 2: Governance and Management of IT, Section 2.3: IT Project Management

NEW QUESTION: 516

□□ □□ □□ □□(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: 517
□□ □ □□□ □□□ □□□ □□□□ □□□ □ □□□ □□ IS □□□□ □□ □□ □□ □□□ □□□□□?
A. □□□ □□
B. □□□
C. □□□□□□(CPU) □□□□
D. □□□□ □□□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 518
□□□ □□□□ □□□□ □□□ □□□ □ IS □□□□ □□ □□□ □□ □□□ □□□ □□□.
A. □□ □□□□□ □□□□ □□□.
B. □□ □□ □□□ □□□□ □ □□□□ □□□□□.
C. □□□□ □□□ □□ □□□ □□□□□.
D. □□□□ □□□□□ □□ □□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 519
IS □□□□ □□□□□ □□ □□ □□□ □□□□ □□□□. □□ □ □□ □□ □□□ □ □□ □□□□ □□□□□ □□ □ □□□ □□□□□?
A. □□ □□ □□□(IDS)
B. □□ □□ □ □□□ □□(SIEM) □□□
C. □□ □□ □□□
D. □□ □□□
Answer: C (LEAVE A REPLY)
A stateful firewall provides the greatest assurance that outgoing Internet traffic is controlled, as it monitors and filters packets based on their source, destination and connection state. A stateful firewall can prevent unauthorized or malicious traffic from leaving the network, as well as block incoming traffic that does not match an established connection. An intrusion detection system (IDS) can detect and alert on suspicious or anomalous traffic, but it does not block or control it. A security information and event management (SIEM) system can collect and analyze logs and events from various sources, but it does not directly control traffic. A load balancer can distribute traffic among multiple servers, but it does not filter or monitor it. References: CISA ReviewManual (Digital Version), Chapter 6, Section 6.2

NEW QUESTION: 520

□□ □□ □□ □□□ □□□□ IS □□□□ □□□□□□□(CIO)□ □□□□ □□ □□ □□□ □□□□ □ □ □□ □□□ □□□□ □□□ □□□□ IS □□□ □□□□ □□□ □□□□□ □□□ □□ □□□. □□□□ □□ □ □□□ □□ □□ □□□?

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

B. □□□□□□□(COO)□□ □□□□ □□ □□ □□□ □□ □□□□□.

C. □□□ □□□□ IS □□ □□

D. □□ □ IS □□ □□ □□

Answer: (SHOW ANSWER)

The auditor should first escalate to audit management to discuss the audit plan. This is because the audit plan should be based on a risk assessment and aligned with the organization's objectives and strategies. The auditor should not accept the CIO's request without proper justification and approval from the audit management, who are responsible for ensuring the audit plan's quality and independence. The auditor should also communicate the potential risks and implications of not conducting IS audits in the upcoming year, such as missing new or emerging threats, vulnerabilities, or compliance issues. References:

* CISA Review Manual (Digital Version), Chapter 2, Section 2.11
* CISA Online Review Course, Domain 1, Module 1, Lesson 22

NEW QUESTION: 521

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

A. □□ □□□□□□ □□

B. □□ □□□ □□

C. □□□□ □□ □□□

D. Agile □□ □□ □□

Answer: B (LEAVE A REPLY)

NEW QUESTION: 522

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

A. □□□ □□ □□□ □□□□ □□□□ □□□□.

B. □□□□ □□ □□□ □□□□ □□□□□.

C. □□□ □□□□ □□□□□□□.

D. □□□□ □□□□ □□ □□□□□.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 523

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

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

NEW QUESTION: 524
□□□□ □□ □□□ □□ □□□ □□□ □ 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: 525
□□□ □□□ □□ □□□□ □□ □□ IS □□□□ □□ □ □□ □□□□□□□ SaaS(Software as a Service) □□□ □□□□ □□□□□. □□□□ □□□ □□□ □□ □□□?
A. IT □□□□ □□□ □□□□ □□□□□□□ □□□□□.
B. □□□ □□□ □□□ □□□□□.
C. □□ □□ □□□ □□□ □□□□□.
D. □□□ □□ □□(SLA)□ □□□□ □□□□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
The auditor should verify whether a right-to-audit clause exists (B) next, because it is a contractual provision that grants the auditor the right to access and examine the records, systems, and processes of the SaaS provider. A right-to-audit clause is important for ensuring transparency, accountability, and compliance of the SaaS provider with the customer's requirements and expectations. A right-to-audit clause can also help the auditor to identify and mitigate any risks or issues related to the SaaS agreement12.
Verifying whether IT management monitors the effectiveness of the environment (A) is not the next step, because it is a part of the ongoing monitoring andevaluation process, not the initial walk-through procedures.

The auditor should first establish the scope, objectives, and criteria of the audit before assessing the performance and controls of the SaaS provider.
Verifying whether a third-party security attestation exists is not the next step, because it is not a mandatory requirement for a SaaS agreement. A third-party security attestation is a report or certificate issued by an independent auditor that evaluates and validates the security controls and practices of the SaaS provider. A third-party security attestation can provide assurance and confidence to the customer, but it does not replace or eliminate the need for a right-to-audit clause3.
Verifying whether service level agreements (SLAs) are defined and monitored (D) is not the next step, because it is not directly related to the audit process. SLAs are contractual agreements that specify the quality, availability, and performance standards of the SaaS provider. SLAs are important for measuring and managing the service delivery and customer satisfaction, but they do not grant or guarantee the right to audit4.

NEW QUESTION: 526
□□ □ □□□ □□ □□ □□□ □□□□ □ □□ □□□ □□ □□□□□?
A. □□□ □□
B. □□□□ □□□ □□
C. □□ □□
D. □□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 527
□□□□ □□□□□□ □□ □ □□□ □□ □□ □□□ □□□ □□□□ □□□ □□□ □□□□ □□□□ □□□ □ □□ □□□ □□□ □□□ □□ □ □□□□□?
A. □□□□□□ □□□ □□□ □□□ □□ □□□ □□□□□ □□□□□.
B. □□□□□ □□□ □□□ □□ □□ □□□□□.
C. 25□ □□□ □□ □ □□□ □□ □□□ □□□ □□□□□.
D. □ □□□□ □□ □□ □□□ □□□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 528
□□ IT □□□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□□□?
A. □□□ □□ □□
B. □□ □□ □□
C. □□ □ □□ □□
D. □□□ □□ □□□(UAT) □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 529
IS □□ □□□ □□□□ □□□ □ □□ □□ □□□ □□□ □ □□ □□□□□?
A. □□ □□□ □□ □□□ □□□
B. □□□ □□□ □□□□□□ □□ □□□ □□ □□□
C. □□ □□ □□ □□□ □□, □□ □ □□
D. □□ □□□ □□ □□□ □□□□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 530
IT □□□□□ □□ □□ □□□ □□□ □□□ □□□ □□□□ □□ □□□□ □□□□ □ □ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□□ □□□ □ □□□ □□ □□, □□□□ □ □□□ □□□□□.
B. □□ □□□□ □□ □□□□□ □□ □□□□ □□ □□□□ □□□□□□.
C. IT □□□ □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□.
D. □□□□ □□□□ □□ □□ □□□ □□□ □ □□ □□□□ □□□ □□□ □□□ □ □□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 531
IS □□□□ IT □□ □□□□ □□□ □□□□ □□□□. □□□ □□, □□□□□ □□ □ □□□ □□□□ □□ □□ □□ □ □□ □□□□?
A. □□□□ □□

B. □□ □□ □□ □□
C. □□ □□□ □□□
D. □□ □□□□ □□ □□□□□
Answer: (SHOW ANSWER)
The missing access control requirements should present the greatest concern to the IS auditor when reviewing a contract for the outsourcing of IT facilities. Access control requirements are essential for ensuring the confidentiality, integrity, and availability of the outsourced IT resources and data. They specify the roles, responsibilities, and permissions of the outsourcing vendor and its staff, as well as the client and its users, in accessing and managing the IT facilities. They also define the security policies, standards, and procedures that the outsourcing vendor must follow to protect the IT facilities from unauthorized or malicious access, use, modification, or disclosure. Without clear and comprehensive access control requirements, the outsourcing contract may expose the client to significant risks of data breaches, compliance violations, service disruptions, or reputational damage.
Hardware configurations, help desk availability, and perimeter network security diagram are important aspects of an outsourcing contract, but they are not as critical as access control requirements. Hardware configurations describe the technical specifications and performance of the IT equipment that the outsourcing vendor will provide and maintain. Help desk availability defines the service levels and support channels that the outsourcing vendor will offer to the client and its users. Perimeter network security diagram illustrates the network architecture and security measures that the outsourcing vendor will implement to protect the IT facilities from external threats. These aspects can be verified or modified during the implementation or operation phases of the outsourcing contract, but access control requirements need to be established and agreed upon before signing the contract.
References:
ISACA, CISA Review Manual, 27th Edition, Chapter 5: Protection of Information Assets, Section 5.3:
Logical Access1
CIO.com, 7 tips for managing an IT outsourcing contract2
Brainhub.eu, 8 Tips for Managing an IT Outsourcing Contract

NEW QUESTION: 532
IS □□□□ □□ □ □□□(PKI)□ □□□ □ □□ □ □□ □□□ □□ □□□ □□ □□□ □□?
A. □□□ □□□□ □□□ □□□(IaaS)□ □□ □□
B. □□□ □□□ □□ □□□ □□□ □□
C. □□□ □□□ □ □ □□ □□ □□ □ □□□□ □□ □□
D. □□ □□□□□ □□ □□□ □□ □ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 533
□□ □ □□□□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□ □□ □□□ □ □□□□?
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: 534
□□ □□□□□□ □□ □□□□ □□ □□□□□ □□□□□?
A. □□□ □□
B. □□□□ □□
C. □□ □□□
D. □□□□ □□□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 535
□□ □□□ □□ IS □□ □□□ □□□□ □□ □ □□□ □□□□□?
A. □□□□□ □□□□□ □□ □ □□ □□
B. □□□□ □□ □□□ □□□□ □□
C. □□ □□□ □□□ □ □□□ □□
D. IS □□ □□□ □□□□ □□□□ □□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 536
□□ □ □□ □□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□□ □□□
B. □□□ □□□ □□□□
C. □□□ □□□
D. □□□ □□
Answer: C (LEAVE A REPLY)
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: 537
□□ □□□ □□ □□ □□□ □□ □□□ □□□ □□□□ □ □□ □□ □□□ □□ □□ □ □□ □ □□□□□?
A. IS □□ □□□□ □□□
B. □□ □□□ □□□ □□ □□
C. □□□ □□ □□ □□
D. □□□□ □□□ □□□□ □□□□□ □□□
Answer: B (LEAVE A REPLY)
The most important determining factor when establishing appropriate timeframes for follow-up activities related to audit findings is the remediation dates included in management responses. The IS auditor should ensure that the follow-up activities are aligned with the agreed-upon action plans and deadlines that management has committed to in response to the audit findings. The follow-up activities should verify that management has implemented the corrective actions effectively and in a timely manner, and that the audit findings have been resolved or mitigated.
The other options are less important factors for establishing timeframes for follow-up activities:
* Availability of IS audit resources. This is a practical factor that may affect the scheduling and execution of follow-up activities, but it should not override the priority and urgency of verifying management's corrective actions.
* Peak activity periods for the business. This is a factor that may affect the availability and cooperation of auditees during follow-up activities, but it should not delay or postpone the verification of management' s corrective actions beyond reasonable limits.
* Complexity of business processes identified in the audit. This is a factor that may affect the scope and depth of follow-up activities, but it should not affect the timeframe for verifying management's corrective actions.

NEW QUESTION: 538
□□ □□□□ □□ □□□ □□□□(IP) □□□ □□□□□ □□ □□ □□□□□ □□□ □ □□ □□□ □□ □ □□□□□?
A. □□ □□□ □□□ □□ □□(DNS) □□□ □□
B. □□□□ □□□□ □ □□□ □□□ □□□ □□□□ □□ □□ □□□ □□

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

NEW QUESTION: 539
□□ □□ □□ □□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□ □□ □□
B. □□ □□□□
C. □□□ □□ □□
D. □□□□□ □□□□
Answer: D (LEAVE A REPLY)
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: 540
□□ □□ □□□ □□ □□□ □ □□□□□□□ □□□ □□□□ □□□□□□ □□□□ □ □□ □□□□ □□ □□□□□?
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: 541
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: 542
IT □□□□□□ □□□ □□□ □□ □□□ □□□□□ □□□ □ □□□□□ □□ □□□ □□ □□□□□?
A. □□□□□(ROI) □□
B. □□□□ □□(EVA)
C. □□□ □□ □□
D. □□ □□ □□(BIA)
Answer: B (LEAVE A REPLY)
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: 543
IS □□□□ □□ □□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□ □?
A. □□□ □□□□ □□□□□□
B. □□□□ □□□□
C. □□ IT □□
D. □□ □□ □□
Answer: B (LEAVE A REPLY)
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: 544
□□ □□ □□ IS □□□□ □□ □□□ □□□ □□□□ □□□□ □ □□□ □□ □□ □ □□ □□□□□. □□□ □□□□ □□□□ □□ □□□ □□ □ □□ □□ □□□□ □□ □?
A. □□ □□ □□(RPO)
B. □□ □□ □□(MTTR)
C. □□ □□□ □□ □□ □□ □□(MAD)
D. □□ □□ □□(KPI)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 545
IS □□□□ □□□□□ □□ □□ IT□□ □□ □□□□ □□ □□ □□□ □□□□ □□□ □□□□□□. □□□□ □□ □□□□ □□□ □□□□.
A. □□ □□□ □□□ □□
B. □□□□ □□ □□□ □□□ □□ □□.
C. □□□ □□□ □□ □□□□ □□ □□
D. □□ □□□□ □□□□ □□ □□□ □□□ □□.
Answer: B (LEAVE A REPLY)
The auditor's primary concern when capacity management for a key system is being performed by IT with no input from the business would be an unanticipated increase in business's capacity needs. This could result in performance degradation, service disruption or customer dissatisfaction if IT is not able to provide sufficient capacity to meet the business demand. Failure to maximize the use of equipment, cost of excessive data center storage capacity or impact to future business project funding are secondary concerns that relate to resource optimization or budget allocation, but not to service delivery or customer satisfaction. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 374

NEW QUESTION: 546
□□□□□ □□ □□□ □□□ □□□□ □ □□□□ □□□ □□□□□□ □□□□ IS □ □□□□ □□ □ □□□□ □□□ □□ □□ □□□□□?
A. □□□ □□□□□ □□ □□□□□ □□□□□ □□ □□□□.
B. □□□□ □□□□□ □□□□□.
C. □□□ □ □□ □□ □□□□ □□□□□□.
D. □□ □□□□ □□□□ □□□□□ □□□□ □□□□.

Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
Ensuring data integrity iscritical, even when handling publicly available information.
* Option A (Incorrect):While tracking system interfaces is useful formonitoring, it is not thegreatest concernif the data being transferred is publicly available.
* Option B (Incorrect):Encryption isimportant, but if the data is alreadypublic, therisk impact is lower compared to data integrity issues.
* Option C (Incorrect):Data interception may not be a critical issue forpublicdata unless it leads to modification or exploitation.
* Option D (Correct):If thedata from the originating system differsfrom the downloaded data, it indicates adata integrity failure. This could result from system errors, transmission faults, or tampering, making it thehighest riskfor an IS auditor to address.
Reference:ISACA CISA Review Manual -Domain 4: Information Systems Operations and Business Resilience- Covers system interfaces, data integrity, and auditing techniques.

NEW QUESTION: 547
□□□ □□□ □□ □□□□□□ IT□ □□□□ □□ □ □□ □□ □ □□□ □□ □ □□ □□□?
A. □□□□ □□□ IT □□□ □□□□ □□ □ □□□□.
B. □□□□ □□□□ □□□ □□□ □□□□ □□ □□ □□□□.
C. IT □□□ □□□□ □□□ □□□□ □□ □ □□□□.
D. IT □□□ □□□ □□□□ □□□□ □□ □ □□□□.
Answer: C (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
IfIT is not involvedinstrategic planning,IT strategy may diverge from business needs, leading to misalignment and inefficiencies.
* Option A (Incorrect):Business strategy alignmentis important, but the greater risk is thatIT investments do not support business goals.
* Option B (Incorrect):Lack of emerging technology awareness is a risk, butIT-business misalignment has broader consequences.
* Option C (Correct):Thegreatest riskis when IT strategyfails to align with business objectives, leading towasted investments, inefficiencies, and competitive disadvantages.
* Option D (Incorrect):IT goals being overlooked is a concern, butmisalignment of IT and business strategies is a more critical risk.
Reference:ISACA CISA Review Manual -Domain 2: Governance and Management of IT- Covers strategic IT alignment and governance best practices.

NEW QUESTION: 548
□□ □ 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: 549
□□□□ □□□ □□ □□ □□ □□□□□□ □ □□ □□□ □□ □ □□□□□?
A. □□□□□ □□□ □□ □□□□ □□ □□ □□□ □□□□.
B. □□ □□□□ □□ □□ □□□ □□□□.
C. □□□ □□□ □□□□ □□□□□.
D. □3□□ □□□□ □□□ □□ □□□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
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: 550
□□□ □□ □□ □□ □□□ □□□□ □□ □□ □□ □□□□□□ □□□□□ □□□ □. IS □□□□ □□□ □□□□ □ □□ □□□ □□ □□ □ □□ □□□□?
A. □□□ □□□ □□ □□ □□ □□
B. □□ □□□ □□ □□ □□ □□□□

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

NEW QUESTION: 551
IS □□□□ □ □□□□□□ □□ □□□(DBMS)□□ □□ □□□□□□ □□ □□□ (DBMS)□□ □□□□ □□ □□□ □□□ □□□□ □□□□. □□ □ □□ □□ □□ □□ □□□□ □□□□ □□□□ □ □□ □□□ □□□?
A. □□□ □□□ □□ □□
B. □□□ □□□ □□ □□
C. □□□ □□□ □□ □□
D. □□□ □□□ □□□□□ □□
Answer: (SHOW ANSWER)
The most helpful thing to ensure the integrity of the system throughout the change when moving from one database management system (DBMS) to another is preserving the same data structure. A DBMS is a software system that manages and manipulates data stored in a database, such as creating, updating, querying, deleting, etc. A database is a collection of structured or organized data that can be accessed or manipulated by a DBMS. A data structure is a way of organizing or arranging data in a database, such as tables, columns, rows, keys, indexes, etc. Preserving the same data structure when moving from one DBMS to another can help ensure the integrity of the system throughout the change, by maintaining the consistency and accuracy of data in the database, and avoiding any errors or issues that may arise from incompatible or inconsistent data structures between different DBMSs. Preserving the same data classifications is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data classifications are categories or labels that define the level of sensitivity or importance of data in a database, such as public, confidential, secret, etc. Data classifications can help protect the security and privacy of data in the database by applying appropriate controls or restrictions on data access or use based on their classifications. Preserving the same data classifications when moving from one DBMS to another can help ensure the integrity of the system throughout the change by preventing unauthorized or inappropriate access or use of data in the database. However, this may not be directly related to the DBMS change, as it may apply to any data migration or transfer process. Preserving the same data inputs is a possible thing to ensure the integrity of the system throughout the change when moving from one DBMS to another, but it is not the most helpful one. Data inputs are sources or methods that provide data to a database, such as user inputs, sensors, files, etc. Data inputs can affect the quality and validity of data in the database by introducing errors or inconsistencies in data entry or collection. Preserving the same data inputs when moving from one DBMS to another can help ensure the integrity of the system throughout the change by reducing errors or inconsistencies in data input or collection.

NEW QUESTION: 552
□□ □□ IS □□□□ □□ □□□□ □□□□ □□□ □□ □ □□□□□□ □□□□ □ □ □□□□□□□ □□□□ □□□□ □ □□□ □□ □□□□□□. □□ □ □□□□ □ □ □□□□ □□□□ □□ □□ □□□□ □□ □□□□□?
A. □□ □□ □□□(IDS)□ □□□□□.
B. □□ □□□ □□□ □□□□□□□.
C. □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□ □□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
The best recommendation to prevent unauthorized access to cloud-based applications and data is to implement multi-factor authentication (MFA). MFA is a method of verifying the identity of a user by requiring two or more pieces of evidence, such as a password, a code sent to a phone, or a biometric factor. MFA adds an extra layer of security to prevent unauthorized access, even if the user's password is compromised or stolen. MFA can also help comply with data privacy and security regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).
The other options are not as effective as MFA in preventing unauthorized access. An intrusion detection system (IDS) is a tool that monitors network traffic and alerts administrators of suspicious or malicious activity, but it does not prevent access by itself. Updating security policies and procedures is a good practice, but it does not ensure that users follow them or that they are enforced. Utilizing strong anti-malware controls on all computing devices can help protect against malware infections, but it does not prevent users from accessing cloud-based applications and data from any Internet-connected web browser.
References:
* ISACA, CISA Review Manual, 27th Edition, 2019, p. 2471
* ISACA, CISA Review Questions, Answers & Explanations Database - 12 Month Subscription2
* What Is Cloud Security? | Google Cloud3
* 5 Cloud Application Security Best Practices | Snyk4

NEW QUESTION: 553
□□ □ □□□ IS □□□□ □□□ □□ □□□ □□□□ □ □□ □□□□ □□□ □□□ □□?
A. □□□ □□ □□□□ □□□□□□ □□□□□.
B. □□ □□□ □□ □□□ □□□□□.
C. □□□□ □□□□□□ □□□□□.
D. □□ □ □□ □□□ □□□□□□.
Answer: C (LEAVE A REPLY)

The most effective way for an organization to help ensure agreed-upon action plans from an IS audit will be implemented is to ensure ownership is assigned. This means that the management of the audited area should accept responsibility for implementing the action plans and report on their progress and completion to the audit committee or senior management. This will ensure accountability, commitment, and follow-up for the audit recommendations34. References: 3: CISA Review Manual (Digital Version), Chapter 1: The Process of Auditing Information Systems, Section 1.6: Reporting, page 41 4: CISA Online Review Course, Module 1:
The Process of Auditing Information Systems, Lesson 1.6: Reporting

NEW QUESTION: 554
□□□□ □□□ □□□□ □□ □□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□ □ □□□□□□. IS □□□□ □□□□ □ □□ □□□ □□□□□ □□□□ □□ □□ □ □ □□□ □□□□ □□□□. □□ □ □□ □□□ □ □□ □□ □□ □□□ □□□□□?
A. □□□ □□ □□ □□□□ □□□□ □□ □□□ □□ □□□ □□ □□□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□□□□ □□□□ □□□□□□□ □□□□□ □□ □□□.
C. □□□ □□□ □□ □□□ □□□□ □□□□ □□ □□□ □□□□□ □□□□□.
D. □□□□□□□ □□ □□□ □□ □□ □□ □□ □□
Answer: (SHOW ANSWER)
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: 555
IS □□□□ □3□ □□□□□ □□□ □□□□□ □□□□ □□□ □□ □□ □□□□ □ □□ □□ □□ □□□□ □□□□ □□□□□. □□ □ □□ □□ □□□□ □□□□□ □ □□□ □ □□□ □□□□ □□ □□□□□□ □□ □□ □□□ □□□□□?
A. □□□ □□ □□(SLA)
B. □□□□ □□ □□ □□
C. □□ □□□ □□□□ □□□□ □□
D. □□ RACI □□
Answer: (SHOW ANSWER)
The best evidence that adequate resources are now allocated to successfully recover the systems is a service level agreement (SLA). An SLA is a contract between a service provider and a customer that defines the scope, quality, and terms of the service delivery.

An SLA should include measurable and verifiable indicators of the service performance, such as availability, reliability, capacity, security, and recovery. An SLA should also specify the roles, responsibilities, and expectations of both parties, as well as the remedies and penalties for non-compliance. An SLA can help to ensure that the third-party vendor has allocated sufficient hardware and other resources to meet the recovery objectives and requirements of the organization. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 556
IS □□□□ □□□ □□ □□□□ □□□□ □□□□□ □ □□□ □□□ □ □□□ □□ □□□□□□. □□ □ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□□ □□□ □□□□.
B. □□□□□ □□ □□□ □□□□□□□□.
C. IT □□□ □□ □□ □□ □□□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best recommendation for an organization that is unable to add new servers on demand in a cost-efficient manner is to build a virtual environment. A virtual environment is a technology that allows multiple virtual machines to run on a single physical server, sharing its resources and capabilities. A virtual environment can help the organization add new servers on demand in a cost-efficient manner by reducing the need for hardware acquisition, maintenance, and power consumption. The other options are not as effective as building a virtual environment, as they do not address the root cause of the problem or provide the same benefits.
Increasing the capacity of existing systems is a short-term solution that can help improve the performance and availability of the current servers, but it does not enable the organization to add new servers on demand in a cost-efficient manner. Upgrading hardware to newer technology is a costly solution that can help enhance the functionality and reliability of the servers, but it does not enable the organization to add new servers on demand in a cost-efficient manner. Hiring temporary contract workers for the IT function is an irrelevant solution that can help supplement the IT staff's skills and knowledge, but it does not enable the organization to add new servers on demand in a cost-efficient manner.
References: CISA Review Manual (Digital Version), Chapter 3, Section 3.3.1

NEW QUESTION: 557
□□ □ IT□ □□□□ □□□ □□□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□ IT □□□□ □□□ □□ □□□□□ □□□ □□
B. IT □□ □□□ □□□□ □□ □□ □□□ □□
C. IT □□ □□□ □□□□ □□□ □□
D. □□□□ □□□□ □□ □□□ □□ □□
Answer: (SHOW ANSWER)
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: 558
□□□ □□□□ □□□□□ □□□□ □□□□ □□□□□□ □□ □□□ □□□□ IS □ □□□ □□ □ □□□□ □□□□□?
A. □□ □□□□□ □□□ □□□ □□□□.
B. □□ □□ □□(OLA)□ □□□□ □□□□□.
C. □□ □□□□□ □□□□ □□ □□□ □□□□□.
D. □□□□□ □□□□□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The greatest concern for an IS auditor reviewing contracts for licensed software that executes a critical business process is that software escrow was not negotiated. Software escrow is an arrangement where a third- party holds a copy of the source code and documentation of a licensed software in a secure location. The software escrow agreement specifies the conditions under which the licensee can access the escrowed materials, such as in case of bankruptcy, termination, or breach of contract by the licensor. Software escrow is important for ensuring the continuity and availability of a critical business process that depends on a licensed software. Without software escrow, the licensee may face significant risks and challenges in maintaining, modifying, or recovering the software in case of any disruption or dispute with the licensor. References:
* CISA Review Manual (Digital Version)
* CISA Questions, Answers & Explanations Database

NEW QUESTION: 559
□□□ □□ □□□□ □□□□ □ □□ □□□ □□□ □□□□ □□□□.
A. □□□ □□ □ □□ □□ □□
B. □□□□ □□□ □□□ □□
C. □□□ □□ □□□ □□□ □□
D. □□□□ □□ □ □□□ □□□ □□
Answer: D (LEAVE A REPLY)
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: 560
□□ □ □□□ □□□ □□□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□□□ □□□□□
B. □□□□ □□ □□(BIA)□□ □□□ □□□□ □□
C. □□ □□ □□□ □□□□ □□
D. □□ □□ □□□ □□ □□ □□□ □□ □□
Answer: A (LEAVE A REPLY)
The primary reason to perform a risk assessment is to determine the current risk profile of the organization, which is the level of risk exposure and the likelihood and impact of potential threats. This will help the organization to identify and prioritize the risks that need to be addressed and to align the risk management strategy with the business objectives. A risk assessment may also help to achieve compliance, support the BIA, and allocate budget, but these are not the primary reasons. References: ISACA Glossary of Terms, section "risk assessment"

NEW QUESTION: 561
□□ □□□□□ □□□ □□ □□ □□□ □□□ □ □□ □□□ □□□ □□□□□□□?
A. □□□
B. □□□□
C. □□
D. □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 562
□□□□ □□□□ □□□□□□ □□□ □ □□□□ □ □□ □□□ □□□ □□ □ □□ □□□□?
A. □ IT □□□□ □□ □□□□ □□
B. □ □□□□ □□□□ □□ □□ □□
C. □□□□□□ □□□□□(NPV)
D. □ □□□□□ □ □□
Answer: C (LEAVE A REPLY)
The most useful metric for management to consider when reviewing a project portfolio is the net present value (NPV) of the portfolio. NPV is a measure of the profitability and value of a project or a portfolio of projects, taking into account the time value of money and the expected cash flows. NPV compares the present value of the future cash inflows with the present value of the initial investment and shows how much value is created or lost by undertaking a project or a portfolio of projects1. A positive NPV indicates that the project or portfolio is worth more than its cost and will generate a positive return on investment. A negative NPV indicates that the project or portfolio is worth less than its cost and will result in a loss. Therefore, NPV helps management to prioritize and select the most profitable and valuable projects or portfolios that align with the organizational strategy and objectives2. The other options are less useful or incorrect because:
* A. Cost of projects divided by total IT cost is not a useful metric for reviewing a project portfolio, as it does not reflect the benefits, value, or return of the projects. It only shows the proportion of IT budget allocated to the projects, which may not be indicative of their strategic importance or alignment3.
* B. Expected return divided by total project cost is not a useful metric for reviewing a project portfolio, as it does not account for the time value of money and the timing of cash flows. It only shows the average return per unit of cost, which may not be comparable across different projects or portfolios with different durations, risks, and cash flow patterns4.
* D. Total cost of each project is not a useful metric for reviewing a project portfolio, as it does not reflect the benefits, value, or return of the projects. It only shows the initial investment required for each project, which may not be indicative of their profitability or viability5. References: Portfolio, Program and Project Management Using COBIT 5 - ISACA, Project Portfolio Management - ISACA, CISA Review Manual (Digital Version), Standards, Guidelines, Tools and Techniques

NEW QUESTION: 563
□□□□ □□□ □□□ □□□□ □□ □□(BIA)□ □□□□ □□ □□□ □□□ □□□□ □?
A. □□□□ □□□ □□□□ □□ □□□ □ □□ □□ □□□ □□□□□.
B. □□ □□□ □□□ □□ □□□ □□ □□□□□ □□□□□.

C. □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□□□ □□□□□.
D. □□□ □ □□□□□□ □□□ □□□□□ □□□□ □ □□□ □□□.
Answer: D (LEAVE A REPLY)
The primary purpose of a Business Impact Analysis (BIA) is to prioritize the restoration of systems and applications (D) based on their criticality to business operations. A BIA assesses the impact of disruptions, identifies critical processes, and determines recovery time objectives (RTOs) and recovery point objectives (RPOs).
Other options:
Identifying legal obligations (A) is an aspect of compliance but not the primary benefit of a BIA.
Providing updates on disaster risk levels (B) falls under risk management rather than BIA objectives.
Delineating employee responsibilities (C) is part of business continuity planning (BCP), not the BIA's main goal.
Reference: ISACA CISA Review Manual, Information Systems Operations and Business Resilience

NEW QUESTION: 564
□□ □□□ □□□□ □□□ □□□ □□□□ □□ □ □□ □□□ □□ □ □□□□□?
A. □□ □□□ □□
B. □□□ □□ □□
C. □□□ □□ □□
D. □□□□ □□ □□
Answer: C (LEAVE A REPLY)
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: 565
□□ □□□□ □□ □□□ □□□ □□ □□□□ □□□ □□ □□ □□□□ □□ □□□ □□□□□□. IT□ □□□ □□□□ □□ □□□□ □□□□ □□□ 2□□ □□ □□□ □ □□ □□□ □□□□□ □□□□□. □□ □ □□ □□ □□□ □□□□□?

A. □□ □□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□ □□□□□.
B. □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□.
C. □□□□ □□□□□□ □□□□ □□ □□ □□□ □□□□□.
D. □□□ □□□□ □□□□ □□ □□ □□□ □□□ □□ □□□□□.
Answer: A (LEAVE A REPLY)
Requiring documentation that the finding will be addressed within the new system is the best course of action for a follow-up audit. An IS auditor should obtain evidence that the complex security vulnerability of low risk will be resolved in the new system and that there is a reasonable timeline for its implementation. The other options are not appropriate courses of action, as they may be too costly, time-consuming, or impractical for a low-risk finding. References:
* CISA Review Manual (Digital Version), Chapter 2, Section 2.5.31
* CISA Review Questions, Answers & Explanations Database, Question ID 209

NEW QUESTION: 566
□□ □□ □□□ □□ □□□□ □□□ □□ □□□ □□□ □□□□□?
A. □□ □□ □□□□□ □□□□ □□□□□.
B. □□ □□ □□□□ □□□□□.
C. □□ □□□ □□□ □□□□□.
D. □□ □□ □□□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
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: 567
□□ □ □□□ □□□□ □□□ □□ IT □□□□ □□□□□ □ □□ □□□ □□ □□□ □□?
A. □□ □□□□ □□□(RPA)
B. □□□ □□□□
C. □□ □□
D. □□□□□□ □□□□(EA)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 568
IS □□□□ □□□ □□ □□□ □□□ □□□□ □□□ □□ □ □□□ □ □□□□.
A. □□□ □□□ □□.

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

NEW QUESTION: 569
□□ □ □□ □□ □□□ □□□□ □□□ □□ □□ □□□ □□□□□ □□□□□?
A. □□□□□□□□ □□□ □□ □□□
B. □□□ □□□ □□□□ □□ □□□ □□ □□
C. □□□ □ □□ □□□ □□
D. □□ □□□ □□□ □□ □□
Answer: (SHOW ANSWER)
The best process for continuous auditing for a large financial institution is validating access controls for real- time data systems. This is because access controls are critical for ensuring the confidentiality, integrity, and availability of the financial data that is processed and transmitted by the real-time data systems. Real-time data systems are systems that provide timely and accurate information to support decision-making and transactions in a dynamic and complex environment. Examples of real-time data systems in the financial sector include payment systems, trading platforms, risk management systems, and fraud detection systems.
Continuous auditing of access controls can help detect and prevent unauthorized access, data leakage, data manipulation, or data loss that could compromise the security, reliability, or compliance of the real-time data systems.
Testing encryption standards on the disaster recovery system is not the best process for continuous auditing for a large financial institution. Encryption standards are important for protecting the data stored or transmitted by the disaster recovery system, which is a system that provides backup and recovery capabilities in case of a disruption or disaster. However, testing encryption standards is not a continuous process, but rather a periodic or event-driven process that can be performed as part of the disaster recovery plan testing or validation.
Performing parallel testing between systems is not the best process for continuous auditing for a large financial institution. Parallel testing is a process of comparing the results of two or more systems that perform the same function or task, such as a new system and an old system, or a primary system and a backup system.
Parallel testing can help verify the accuracy, consistency, and compatibility of the systems. However, parallel testing is not a continuous process, but rather a temporary or transitional process that can be performed as part of the system implementation or migration.
Validating performance of help desk metrics is not the best process for continuous auditing for a large financial institution. Help desk metrics are indicators that measure the efficiency, effectiveness, and quality of the help desk service, which is a service that provides technical support and assistance to the users of information systems and technology. Help

desk metrics can include metrics such as response time, resolution time, customer satisfaction, and service level agreement (SLA) compliance. Validating performance of help desk metrics can help evaluate and improve the help desk service. However, validating performance of help desk metrics is not a continuous auditing process, but rather a continuous monitoring process that can be performed by the help desk management or quality assurance team.
References:
* All eyes on: Continuous auditing - KPMG Global 1
* Internal audit's role at financial institutions: PwC 2
* The Fed - Supervisory Policy and Guidance Topics - Large Banking ... 3
* Continuous Audit: Definition, Steps, Advantages and Disadvantages 4

NEW QUESTION: 570
□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□ IS □□□ □ □□ □□ □□□ □□ □□□?
A. □ □□ □□□ □□ □□□ □□□□□.
B. □3□□□ □□□□ □□□□□ □□□□□.
C. □□□ □□□ □□□ □□ □□□.
D. □□ □□ □□□ □□ □□□ □□□□.
Answer: D (LEAVE A REPLY)
The IS auditor should notify audit management of the finding first, as this is a significant issue that may affect the audit scope and objectives. The IS auditor should not notify law enforcement or require the third party to notify customers without consulting audit management first. The audit report with a significant finding should be issued after the audit is completed and the findings are validated. References: ISACA, CISA Review Manual, 27th Edition, 2018, page 247

NEW QUESTION: 571
□□□ □□□ □□ □ □□□ □□□□□□ □□□ □□□ □ IS □□□□ □□□□ □ □ □ □□□ □□□ □□□□□?
A. □□□: □□□ □□□□□□□.
B. □□ □□□ □□□□ □□□□.
C. □□ □□ □□□ □□□□ □□□□.
D. □□ □□ □□□□ □□□□□□□.
Answer: (SHOW ANSWER)
The most important thing for an IS auditor to verify when evaluating an organization's data conversion and infrastructure migration plan is that a rollback plan is included. A rollback plan is a contingency plan that describes the steps and actions to be taken in case the data conversion or infrastructure migration fails or causes unacceptable problems or risks. A rollback plan can help to restore the original data and infrastructure, minimize the impact on the business operations and functions, andensure the continuity and availability of the

IT services. The IS auditor should verify that the rollback plan is feasible, tested, documented, and approved, and that it covers all the possible scenarios and outcomes of the data conversion or infrastructure migration. Theother options are not as important as verifying the rollback plan, because they either do not address the potential failure or disruption of the data conversion or infrastructure migration, or they are partof the normal planning and execution process rather than a contingency plan. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

NEW QUESTION: 572
□□ □□ □□ □ □□ □□ □□ □□□ □□□ □□ □□(DLP) □□□ □□□ □ □□□ □□□?
A. □□ □□□□ □□□(RPA)
B. □□□□ □□□□
C. □□□□□(IoT)
D. □□□□ □□□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 573
□□□ □□ □□ □□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □□□□ □?
A. □□ □□□ □□□ □□□ □□□□□ □□□□□.
B. □□ □□ □□□ □□ □□□□ □□□□.
C. □□□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.
D. □□ □□□□ □□ □□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 574
IS □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□□ □□□□ □□ □ □□ □□□ □□□□ □□ □□□ □□ □□ □□□(IDS)□ □□□□ □□□□.
A. □□□ □ □□.
B. □□□.
C. □□□ □□□□.
D. □□□□□(DMZ).

Answer: B (LEAVE A REPLY)

NEW QUESTION: 575
IS □□□□ □□ □□ □□□ □□□ □ □□ □□□□ □□□□ □ □□□ □□□□□?
A. □□ □□ □□□ □□ □□ □□□(CAE)□ □□□ □□ □□□□□.
B. □□□□□□□□ □□□□□ □□□ □□□□ □□ □□□□.
C. □□ □□ □□□ □□ □□□□ □□□□.
D. □□□□□□□ □□□□□□ □□ □□□□ □□□□□.
Answer: D (LEAVE A REPLY)
The auditor should be most concerned about the information security policy not being approved by the policy owner. This is because the policy owner is the person who has the authority and accountability for ensuring that the policy is implemented and enforced. Without the policy owner's approval, the policy may not reflect the organization's objectives, risks, and compliance requirements. The policy owner is usually a senior executive or a board member who has a stake in the information security governance. The other options are less critical than the policy owner's approval, although they may also indicate some weaknesses in the policy development and maintenance process.
References:
* CISA Review Manual (Digital Version), Chapter 1, Section 1.21
* CISA Online Review Course, Domain 5, Module 1, Lesson 12

NEW QUESTION: 576
□□ □ 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: 577

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

NEW QUESTION: 578
□□□ □□□□□ □□ □□ □□ □□ □□□ □□ □□ □□ □□□□□ □□□□ □□ □□ □□□ □□□ □□□□□. □□ □ □□ □□ □□□ □□ □□ □□ □□ □□□ □□ □□ □ □□ □□□□□?
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: 579
□□ □ □□ □□□ □□ □□ □□□ □□ □□□ □□□□□?
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: 580
□□ □ □□□□□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□ □□ □□ □□ □□ □□ □□□ □□□□□?
A. □□ □□ □□
B. □□□ □□□
C. □□□ □□
D. □□□ □□□ □□
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed Step-by-Step Explanation:
Thebest protectionfor a stolen laptop isfull disk encryption, which prevents unauthorized accesseven if the device is lost.
* Option A (Incorrect):Remote wipe capabilitiesare useful, but theyrequire an internet connectionto function, which is not always available when a device is stolen.
* Option B (Correct):Full disk encryption (FDE)ensures that data remainsunreadablewithout the correct decryption key,even if the hard drive is removed.
* Option C (Incorrect):User awarenessis helpful, but itdoes not physically securedata on a lost device.
* Option D (Incorrect):Password-protected filescan be bypassed by copying them to another system, making them an inadequate security measure.
Reference:ISACA CISA Review Manual -Domain 5: Protection of Information Assets-Covers encryption, data security, and endpoint protection.

NEW QUESTION: 581
IS □□□□ □□□□□□ □□ □□ □□ □ □□ □□□□ □□□□ □□□ □□ □ □□ □□□?

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

NEW QUESTION: 582
□□ □ □□ □□□ □□□ □□ □ □□ □□ □□□ □□□ □□ □□□ □□□ □ □□ □□ □ □□□ □□□□ □□ □□□□□?
A. □□ □□□ □□ □□(SLA)□ □□□□ □□ □□□ □□
B. □□□□□□ □□□ □□□□ □□□ □□□□□ □□ □□
C. □□□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□ □□
D. □□ □□ □□□ □□ □□ □□ □□ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 583
□□ □□ IS □□ □□□□□ □□□ □ IS □□□□ □□ □□□ □□□ □ □□□ □□□ □□?
A. □□□□□ □□
B. □□ □□
C. □□□□ □□□□
D. IT □□ □□
Answer: (SHOW ANSWER)
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: 584
□□□ □□ □□□□ □□□□□ □□□□□. □□ □□ □ □□□ □□ □□ □□□ □□ □□ IS □□□□ □□ □□□□ □□□ □□ □ □□ □□□□?
A. □□□□□□ □ □□ □□ □□(DRP) □□□□ □□□□□□ □□□ □□□□.
B. □□□□ □□□ □□□□ □□ □□□□ □□□□□ □□□ □□□□ □□□□□□□.
C. □□ □□ □ □□□□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□□□.

D. □□□□□□ □ □□ □□ □□(DRP)□ □□□ □□ □□□□□ □□□□□□ □□□ □□.

Answer: A (LEAVE A REPLY)

After migrating infrastructure to the cloud, it's imperative to test the disaster recovery plan (DRP) to ensure its effectiveness in the new environment. Without evidence of DRP testing post-migration, the organization cannot be certain that it can recover and continue operations during a disaster. While updating the DRP and configuring redundancy are essential steps, their effectiveness can only be validated through rigorous testing. Retaining previous infrastructure is less relevant if the cloud environment is properly configured and tested for disaster recovery.

References:

* ISACA CISA Review Manual, 28th Edition, Chapter 4: Information Systems Operations and Business Resilience.

NEW QUESTION: 585

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

A. □□ □□ □□□ □□□□□.

B. □□ □□□ □□ □□□ □□□□□

C. □□ □□□ □□□□ □□□ □□□□□.

D. □□□ □□ □□(MDM) □□□□□ □□□ □□

Answer: B (LEAVE A REPLY)

The first thing that should be done before allowing users to connect personal devices to the corporate network is to implement an acceptable use policy. An acceptable use policy is a document that defines the rules and guidelines for using personal devices on the corporate network, such as security requirements, access rights, responsibilities, and consequences. An acceptable use policy can help to protect the organization from potential risks such as data leakage, malware infection, or legal liability. The other options are not as important as implementing an acceptable use policy, as they do not establish the boundaries and expectations for using personal devices on the corporate network.

References: CISA Review Manual, 27th Edition, page
318

NEW QUESTION: 586

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

A. □□□□ □□ □□□ □□□□□.

B. □□□□□ □□□ □□□ □□□□□.

C. □□□□ □□□ □□□□□.

D. □□ □□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

The most effective way to maintain network integrity when using mobile devices is to implement network access control. Network access control is a security control that regulates and restricts access to network resources based on predefined policies and criteria, such as device type, identity, location, or security posture.
Network access control can help maintain network integrity when using mobile devices by preventing unauthorized or compromised devices from accessing or affecting network systems or data. The other options are not as effective as network access control in maintaining network integrity when using mobile devices, as they do not address all aspects of network access or security. Implementing outbound firewall rules is a security control that filters and blocks network traffic based on source, destination, protocol, or port, but it does not regulate or restrict network access based on device characteristics or conditions. Performing network reviews is a monitoring activity that evaluates and reports on the performance, availability, or security of network resources, but it does not regulate or restrict network access based on device characteristics or conditions. Reviewing access control lists is a verification activity that validates and confirms the access rights and privileges of network users or devices, but it does not regulate or restrict network access based on device characteristics or conditions. References: CISA Review Manual (Digital Version), Chapter 5, Section
5.2.2

NEW QUESTION: 587
□□ □ □□ □□ □□ □□□ □□ □ □□□□□ □□□□ □□□ □□ □□□□ □□□ □ □□ □ □□□ □ □□□□?
A. □□ □□ □□□
B. □□ □□ □□
C. □□ □□ □□(CSA)
D. □□ □□ □□
Answer: B (LEAVE A REPLY)
Quality control reviews are the best way to demonstrate to senior management and the board that an audit function is compliant with standards and the code of ethics. Thesereviews assess the efficiency and effectiveness of the audit function, ensure compliance with audit standards and ethics, and identify areasfor improvement12. While audit staff interviews, control self-assessments (CSAs), and corrective action plans can

provide valuable insights, they do not offer the same level of assurance as a comprehensive quality control review12.
References: The Institute of Internal Auditors1, AuditBoard2

NEW QUESTION: 588
□□ □ □□□ □□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□□□□ IT □□□ □□□□□ □□
B. □□ □□□ □□□□□□ □□
C. □□□□□ □□□ □□ □□□ □□□□□□ □□
D. □□ □□□ □□□□□□□ □□
Answer: (SHOW ANSWER)
The most important thing to determine when conducting a post-implementation review is whether success criteria have been achieved. A post-implementation review is a process of evaluating the results and outcomes of a project or initiative after it has been completed and implemented. The success criteria are the measurable indicators that define what constitutes a successful project or initiative in terms of its objectives, benefits, quality, performance, and stakeholder satisfaction. The IS auditor should verify whether the success criteria have been achieved by comparing the actual results and outcomes with the expected or planned ones, and by assessing whether they meet or exceed the expectations and requirements of the stakeholders. The IS auditor should also identify any gaps, issues, or risks that may affect the sustainability or scalability of the project or initiative, and provide recommendations for improvement or remediation. The other options are not as important as determining whether success criteria have been achieved when conducting a post- implementation review, because they either focus on specific aspects or components of the project or initiative rather than theoverall value proposition, or they are part of the pre-implementation or implementation phases rather than the post-implementation phase. References: CISA Review Manual (Digital Version)1, Chapter 4, Section 4.2.3

NEW QUESTION: 589
□□ □ □□ □ □□□ □□ □□□□ □□ □□□ □□□□□?
A. □□□□□□, □□ □ □□□□ □□ □□ □□ □□□ □□
B. □□□ □□ □□□ □□□ □□ □□ □□ □□ □□
C. □□ □□□ □□□ □□
D. □□□□ □□□ □□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 590
□□ □ IS □□□□ □□ □□□ □□□(EUC) □□□ □□ □□ □□ □□□□□□□ □□ □□□ □□□ □ □□ □□□ □□ □□□□□?
A. □□ □□□ □□ □□□□□□ □□

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

NEW QUESTION: 591
□□□□□□ □□□ □□□□ □□ IS □□□□ □□□□□□ □□□(DBA) □□□ □□ □□ □□□ □□□ □□ □□□ □□□ □□ □□ □□□□□ □□□□ □□ □□ □□□ □□□. □□□□ □□ □ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□□ □□□□□.
B. IT □□□□□ □□□ □□ □□□□□ □□□□ □□□ □□□□□□□ □□□□□.
C. □□ □□□ □□□□□ □□□□ □□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□.
Answer: C (LEAVE A REPLY)
The auditor's best course of action is to document the finding and explain the risk of having administrator accounts with inappropriate security settings. This is because the auditor's role is to identify and report the issues, not to fix them or request others to fix them. The auditor should also communicate the impact of the finding, such as the possibility of unauthorized access, data tampering, or denial of service attacks. The auditor should not assume the responsibility of the IT manager or the DBA, who are in charge of changing the security parameters or disabling the accounts. References:
* CISA Review Manual (Digital Version), Chapter 4, Section 4.2.21
* CISA Online Review Course, Domain 1, Module 3, Lesson 32

NEW QUESTION: 592
□□ □□ □□ □ □□ □□□ □□□□□□ □□□□□ □□□□ □□□□ □□□ □□ □□ □□□□ □□□ □ □ □□□□?
A. □□ □□ □□ □□
B. □□□ □□□
C. □□ □□
D. □□□□ □□ □□
Answer: A (LEAVE A REPLY)
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: 593
□□ □ IT □□□ □□ □□□ □□□□ □□ □□ □ □□□□ □□ □□□□□?
A. IT □□ □□ □□
B. □□ □□□□□ 2□□□ □□
C. □□ □□□ □□
D. □□□ □□□□□ □□
Answer: (SHOW ANSWER)
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: 594
□□□ □□ □□□□ □□ □□ □□□□ □ □□□ □□□□□?
A. □□□ □□ □□□
B. □□ □□□
C. □□□□
D. □□ □□ □□
Answer: C (LEAVE A REPLY)

The risk assessment process involves identifying the information assets that are at risk, analyzing the threats and vulnerabilities that could affect them, evaluating the impact and likelihood of a risk event, and determining the appropriate controls to mitigate the risk. The first step is to identify the information assets, as they are the objects of protection and the basis for the rest of the process. Without knowing what assets are at risk, it is not possible to assess their value, exposure, or protection level. References: ISACA Frameworks: Blueprints for Success

NEW QUESTION: 595
□□□ □□ □□□□ □□□ □□ □□□ □□□ □□□□ IS □□□□ □□ □□□□ □ □□□ □□ □ □□□□□?
A. □□□ □□ □□□□ □□ □□□ □□□□□.
B. □□ □□ □□□□□□ □□ □□□(VPN) □□□ □□□□□ □□ □□□□.
C. □□ □□ □□□ □□□ □□ □□(MDM)□ □□□□ □□ □□□□.
D. □□ □□ □ □□ □□□ □□□□ □□□ □ □□ □□□□ □□□ □ □□□□.
Answer: (SHOW ANSWER)
Comprehensive and Detailed Step-by-Step Explanation:
A lack ofMobile Device Management (MDM) enrollmentis the biggest concern, asunmanaged devices pose a serious security risk.
* Not All Devices Enrolled in MDM (Correct Answer - C)
* Unenrolled devices can bypass security policies.
* Example:A stolen, unenrolled device may lack encryption, exposing corporate data.
* Biometric Authentication Required (Incorrect - A)
* Biometrics are anenhanced security measure, not a concern.
* VPN Not Required for Internal Network (Incorrect - B)
* VPNs are typically used for external access, not always needed internally.
* Remote Wipe Requires Internet (Incorrect - D)
* A limitation but stillless riskythan allowing unsecured devices.
References:
* ISACA CISA Review Manual
* NIST 800-124 (Mobile Device Security)

NEW QUESTION: 596
□□□□□□□ □□□□ □ □□□ □□□ □ IS □□□□ □□□□□□□ □□□□□ □ □□□□□. □□□□ □□□ □□□□ □□□.
A. □□ □□□ □□□ □□ □□□ □□□□□.
B. □□□□□□□ □□□ □□□ □□□ □□□□□.
C. □□ □□□□□ □□□ □□□□□ □□□ □□□□.
D. □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

The IS auditor should inform audit management of the earlier involvement in designing the application. This is to ensure that there is no conflict of interest or bias that may affect the objectivity or independence of the audit. Audit management can then decide whether to assign a different auditor or to proceed with the same auditor with appropriate safeguards. The other options are not appropriate for the IS auditor to do in this situation. Refusing the assignment to avoid conflict of interest is an extreme measure that may not be necessary or feasible, especially if there are no other qualified auditors available. Using the knowledge of the application to carry out the audit is risky, as it may lead to overlooking or ignoring potential issues or errors in the application. Modifying the scope of the audit is not advisable, as it may compromise the quality or completeness of the audit. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.1

NEW QUESTION: 597

□□ □□□□ □□ □□□ □3□□ □□□□□ □□ □□ □□□□□□□ □□□□ □□ □ □□□□ □□□□.

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

A. □□□ □□□ □□□ □□ □□

B. □□□□□□□ □□□□□ □□□ □□ □□□ □□□ □□

C. □□□ □□□ □□□ □□□□ □□ □□

D. □□□ □□□ □□□□ □□□□ □□ □□□□ □□ □□

Answer: C (LEAVE A REPLY)

This is because privacy regulations are laws or rules that protect the personal information of individuals from unauthorized access, use, disclosure, or transfer by third parties. Payroll audit documentation may contain sensitive and confidential data, such as employee names, salaries, benefits, taxes, deductions, and bank accounts. If the audit management application is hosted by a third party in a different country, the organization may need to comply with the privacy regulations of both its own country and the host country, as well as any international or regional agreements or frameworks that apply. Privacy regulations may impose various requirements and obligations on the organization, such as obtaining consent from the data subjects, implementing appropriate security measures, notifying data breaches, and ensuring data quality and accuracy.

Privacy regulations may also grant various rights to the data subjects, such as accessing, correcting, deleting, or transferring their data. Failing to comply with privacy regulations may expose the organization to significant risks and consequences, such as legal actions, fines, sanctions, reputational damage, or loss of trust.

Some examples of privacy regulations affecting the organization are:

* The General Data Protection Regulation (GDPR), which is a comprehensive and strict privacy regulation that applies to any organization that processes personal data of individuals in the European Union (EU) or offers goods or services to them, regardless of where the organization or the data is located1.

* The California Consumer Privacy Act (CCPA), which is a broad and influential privacy regulation that applies to any organization that collects personal information of California residents and meets certain thresholds of revenue, data volume, or data sharing2.
* The Health Insurance Portability and Accountability Act (HIPAA), which is a sector-specific privacy regulation that applies to any organization that handles protected health information (PHI) of individuals in the United States, such as health care providers, health plans, or health care clearinghouses3.
Therefore, before using an audit management application hosted by a third party in a different country, the internal audit team should conduct a thorough assessment of the privacy regulations affecting the organization and ensure that they have adequate policies, procedures, and controls in place to comply with them.

NEW QUESTION: 598
□□□ □□ □□ □□□ □□□ □ □□ □□ □□□□ □□□□ □□□ □□□ □□ □□ □ □□ □□ □□□□ □□ □□□ □□□□□?
A. □□□ □□ □□□ □□ □□ □□□□ □□□ □□□□ □□ □□ □□□□□.
B. □□□□ □□□□ □□ □□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□.
C. □□□ □□ □□□ □□ □□ □□□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□.
D. □□□ □□, □□, □□□ □□□□□ □□□ □□□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 599
□□ □□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□□□□?
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: 600

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

A. □□ □□ □□□

B. □□ □□□□ □□□□ □□

C. □□ □□ □□□

D. □□ □□□□ □□□□ □□

Answer: B (LEAVE A REPLY)

Stratified mean per unit sampling is a method of audit sampling that divides the population into subgroups (strata) based on some characteristic, such as monetary value, and then selects a sample from each stratum using mean per unit sampling. Mean per unit sampling is a method of audit sampling that estimates the total value of a population by multiplying the average value of the sample items by the number of items in the population. Stratified mean per unit sampling is suitable for populations that have a high variability or a skewed distribution, such as the bank accounts in this question. By stratifying the population, the auditor can reduce the sampling error and increase the precision of the estimate.

Difference estimation sampling (option A) is not the best sampling approach for these accounts. Difference estimation sampling is a method of audit sampling that estimates the total error or misstatement in a population by multiplying the average difference between the book value and the audited value of the sample items by the number of items in the population. Difference estimation sampling is suitable for populations that have a low variability and a symmetrical distribution, which is not the case for the bank accounts in this question.

Customer unit sampling (option C) is not a sampling approach, but a type of monetary unit sampling.

Monetary unit sampling is a method of audit sampling that selects sample items based on their monetary value, rather than their physical units. Customer unit sampling is a variation of monetary unit sampling that treats each customer account as a single unit, regardless of how many transactions or balances it contains.

Customer unit sampling may be appropriate for testing existence or occurrence assertions, but not for estimating total values.

Unstratified mean per unit sampling (option D) is not the best sampling approach for these accounts.
Unstratified mean per unit sampling is a method of audit sampling that applies mean per unit sampling to the entire population without dividing it into subgroups. Unstratified mean per unit sampling may result in a larger sample size and a lower precision than stratified mean per unit sampling, especially for populations that have a high variability or a skewed distribution, such as the bank accounts in this question.
Therefore, option B is the correct answer.
References:
* Audit Sampling - AICPA
* Audit Sampling: Examples and Guidance To The Sampling Methods
* Audit Sampling |Audit | Financial Audit - Scribd

NEW QUESTION: 601
□□ □ IT □□ □□□ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□□□?
A. □□□ □□ □□□ □□□ □□
B. □□ □□□ □□□ □□ □□
C. □□□ □□ □ 0t
D. □□□ □□ □
Answer: D (LEAVE A REPLY)
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: 602
□□□ □□□□ □□□□ □□ IS □□□□ □□ □□□□ □□□ □□ □□ □□□ □□ □□□ □□□□ □□□. □□□ □□□ □□ □□ □□ □□□ □□ □ □□□□□?
A. □□ □□ □□
B. □□□ □□□ □□□□□ □□□□□.
C. □□ □□□□□□ □□□ □□ □□□□□.
D. □□□ □□ □□(UAT) □□ □□
Answer: C (LEAVE A REPLY)
The best way to obtain assurance that certain automated calculations comply with the regulatory requirements is to re-perform the calculation with audit software. This will allow the auditor to independently verify the accuracy and validity of the calculation and compare it with the expected results. Reviewing sign-off documentation, source code, or user acceptance test results may not provide sufficient evidence or assurance that the calculation is correct and compliant. References:
* CISA Review Manual (Digital Version), page 325
* CISA Questions, Answers & Explanations Database, question ID 3335

NEW QUESTION: 603
IS □□□□ □□□□□□□ □□ □□□ □□□ □□ □□□□ □□□.
A. □□□ □□□□□.
B. □□ □□□□□□ □□□□ □□□□□.
C. □□□□□ □□ □□□□□
D. □□ □□□□ □□□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
An application's audit trail is a record of all actions or events that occur within or affect an application, such as user activities, system operations, data changes, errors, exceptions, etc. An audit trail can provide evidence and accountability for an application's functionality and performance, and support auditing, monitoring, troubleshooting, and investigation

purposes. An IS auditor should ensure that an application's audit trail has adequate security, which means that it is protected from unauthorized access, modification, deletion, or disclosure. Adequate security can help ensure that an audit trail maintains its integrity, reliability, and availability, and prevents tampering or manipulation by attackers or insiders who want to hide their tracks or evidence of their actions. Logs all database records is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as logging all database records may not be necessary or feasible for some applications, and may generate excessive or irrelevant data that can affect the storage or analysis of the audit trail. Is accessible online is a possible feature of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as online accessibility may not be required or desirable for some applications, and may introduce security or privacy risks for the audit trail. Does not impact operational efficiency is a desirable outcome of an application's audit trail, but it is not the most important thing for an IS auditor to ensure, as operational efficiency may not be the primary objective or concern of an application's audit trail, and may depend on other factors or trade-offs such as storage capacity, performance speed, or data quality.

NEW QUESTION: 604
IS □□□□ □□□ □□□□□□ □□ □□□ □□ □□□ □□□ □□□□ □ □□ □ □ □ □□□□□□. □□ □ □□□ □□□ □□□□ □ □□ □□□ □□□ □□□ □□□□ □?
A. □□□ □□□
B. □□□ □□□
C. □□□ □□□
D. □□□ □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 605
□□□ □□□ □□ □□ □□□ □□□□ IS □□□□ □□□ □□ □□ □□ □□□ □□ □□.
A. □□□ □□ □ □□□ □□□ □□□□ □□□□.
B. □□□ □□ □□□□ □□ □□□□ □□□ □□□□.
C. □ □□□ □□ □□□□ □□ □□□□□□□.
D. □□ □□□ □□□ □□□□□□□.
Answer: (SHOW ANSWER)
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: 606
□□ □□ □□ IS □□□□ □□□□□□ □□ □□ □□□(IPS)□□ □□ □□ □□□ □ □□□ □□□ □□□□. □□□□ IPS □□□ □□□ □□□ □ □□ □□□ □□□ □□□ □ □□ □□□□ □□□ □□ □□□ □□□□□?
A. □□□ □□
B. □□ □□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)
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: 607
□ □□□ □□ □□ □□□ □□□□□□ □□□ □□□□□ □□□□□ □□ □□□□□ □□□□□□□□□□. □□ □ □□□ □□□ □□□□□ □□□□ IS □□□□ □□ □□ □□ □ □□□ □□□□□?
A. □□□□ □□ □□□ □□□ □□□□□.
B. □□□□ □□□□□□□□□□ □□□□ □□ □□□□ □□□□ □□□□□.
C. □□□□□□ □□□□ □□□ □□□ □□ □□□ □□□ □□ □□□□□.
D. □□□□ □□□ □□□□□□ □□□□□ □□□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 608
IS □□□□ □□ □□□□□ □□ □□□□ □□ □□□ □□ □□□□□ □□□□ □□□ □. □□ □□□□ □□□□□ □□□ □□□□□ □□□ □□□□ □□ □□□□?
A. □□□□
B. □□□
C. □□
D. □□
Answer: A (LEAVE A REPLY)
A staging environment is a replica of the production environment that is used to test and verify software before deploying it to production. A staging environment is most likely to have the same software version as production, as it mimics the real-world conditions and configurations that will be encountered in production.
A testing environment is a separate environment that is used to perform various types of testing on software, such as functional testing, performance testing, security testing, etc. A testing environment may not have the same software version as production, as it may undergo frequent changes or updates based on testing results or feedback. An integration environment is a separate environment that is used to combine and test software components or modules from different developers or sources, to ensure that they work together as expected.
An integration environment may not have the same software version as production, as it may involve different versions or branches of software from different sources. A development environment is a separate environment that is used by developers to create and modify software code. A development environment may not have the same software version as production, as it may contain unfinished or untested code that has not been released yet.

NEW QUESTION: 609
□□□ □□□ □, □□□□ □□ □□□ □□□□□ □ □□□ □□□ □□□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□□?
A. □□ □□
B. □□ □□
C. □□ □□ □□
D. □□□□□□
Answer: A (LEAVE A REPLY)
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: 610
□□□ □□ □□□ □□□ □ □□ □□□ □ □□ □□, □□ □ □□ □□ □□□□ □ □ □□ □□□□□?
A. □□□ □□□ □□□□□.
B. □□ □□□□ □□□□□.
C. □□□ □□□□□.
D. □□ □□□ □□□□□□.
Answer: D (LEAVE A REPLY)
In the event of a disaster where the data center is no longer available, the first step should be to activate the call tree1. A call tree is a layered hierarchical communication model used to notify specific individuals of an event and coordinate recovery efforts1. This ensures that all relevant parties are informed about the situation and can begin executing their parts of the disaster recovery plan1.
References:
IT Disaster Recovery Plan | Ready.gov

NEW QUESTION: 611
□□ □ □□ □□□□ □□ □□□ □□ □□□□ □□□□ □□□□ □□□ □□ □□ □ □□□ □□□ □ □ □□□□?
A. □□ □□□ □□ □□ □□ □□
B. □□ □□ □ □□ □□

C. □□ □□ □ □□ □□ □□

D. □□□ □□ □ □□ □□

Answer: (SHOW ANSWER)

The best test to provide assurance that a health care organization is handling patient data appropriately is compliance with local laws and regulations, as these are the primary sources of authority and obligation for data protection and privacy. Compliance with action plans, industry standards, or organizational policies and procedures are also important, but they may not cover all the legal requirements or reflect the currentbest practices for handling patient data. References: CISA Review Manual (Digital Version), Chapter 2, Section
2.3

NEW QUESTION: 612

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

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: 613

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

A. □□□ □□ □□□ □□□ □□ □□ □□(SDLC)□ □□

B. □□□□ □□□ □□□□□ □□□□ □□ □□□ □□□ □□

C. □□□ □□□ □□□ □□□□ □□ □□□ □□ □□ □□

D. □□□□ □□□ □□ □□□□ □□□□□□□ □□□□□.

Answer: A (LEAVE A REPLY)

A data warehouse is a centralized repository of data that is collected from various sources and organized for analysis and reporting purposes. A data warehouse can help an

organization gain insights into its business performance, trends, and opportunities. However, building a data warehouse requires careful planning, design, and implementation to ensure that it meets the needs of the organization.
One of the best practices that would provide management with the most reasonable assurance that a new data warehouse will meet the needs of the organization is A. Integrating data requirements into the system development life cycle (SDLC). The SDLC is a framework that defines the phases and activities involved in developing a software system, such as planning, analysis, design, testing, deployment, and maintenance1. By integrating data requirements into the SDLC, an organization can ensure that the data warehouse is aligned with the business objectives and expectations, and that it delivers value to the end users.
Some of the benefits of integrating data requirements into the SDLC are:
It helps to identify and prioritize the key business questions and metrics that the data warehouse should support2.
It helps to define and validate the data sources, models, structures, and quality standards that the data warehouse should follow3.
It helps to design and implement the data integration, transformation, and loading processes that the data warehouse should use4.
It helps to test and verify the functionality, performance, and accuracy of the data warehouse before deploying it to production.
It helps to monitor and maintain the data warehouse after deployment and incorporate feedback and changes as needed.

NEW QUESTION: 614
IS □□□□ □□□□ □□□□□ □□□□ □□□□ □□□, □□□□ □□□□ □□□□ □□ □□ □□□ □□□□□□ □□□□□ □□□ □□ □□□□□. □ □□□□ □□□ □ □□ □□ □□□ □□□ □□ □ □□ □□□□?
A. □□□□ □□□□ □□
B. □□ □□□□□□ □□□
C. □□ □□ □□ □□
D. □□ □□□□□□□ □□ □□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 615
□□ □ □□ □□□□ □□ □□□□□ □□□□ □□ □□ □□□□□□ □□□ □□□ □□□ □□□□ □□ □□□□?
A. □□□ □□ □□□(UAT)
B. □□ □□□
C. □□□□ □□□
D. □□□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 616
□□ □□ □□ □□ IS □□□□ □□ □□□ □□ □□ □□□ □□ □□ □ □□ □□ □ □ □□□ □□□□ □□□ □□ □□ □□□. 1□ □□□ □□□ □□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□□ □□ □□ □□ □□□ □□□□□?
A. □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□□□□ □□□.
B. □□□ □ □□ □□□ □□□□□ □□□ □□□□□.
C. □□ □□□ □□□□ 6□□□□ □□ □□□ □□□□□□ □□□ □□□□□.
D. □□ □□ □□□□□ □□ □□□ □□ □□□ □□□□□ □□□□□.
Answer: B (LEAVE A REPLY)
This directly addresses the gap for new hires, creates a consistent expectation regardless of hiring date, and formalizes the process within organizational policy.
References
ISACA CISA Review Manual (Current Edition) - Chapters on Information Security Policies, Training and Awareness Industry Best Practices for Security Awareness - Emphasize the importance of timely and comprehensive training for new employees.

NEW QUESTION: 617
IS □□□□ □□ □□ □□□ □□ □□□□ □□□ □□□ □□□ □ □□□□ □ □□ □ □□ □□□ □□□□□?
A. □□□□□ □□□□□ □□ □□ □□□□ □□□ □□□□□.
B. □□□□ □□□□□ □□ □□□□ □□□□ □□ □□□□□.
C. □□ □□□□□ □□□ □□ □□□ □□□ □□ □□□□.
D. □□□ □□ □□□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
The most important thing for an IS auditor to verify when reviewing the use of an outsourcer for disposal of storage media is that the vendor's process appropriately sanitizes the media before disposal. As explained in the previous question, storage media may contain sensitive or confidential information that needs to be protected from unauthorized access, disclosure, or misuse. The IS auditor should verify that the vendor has a process that appropriately sanitizes the media before disposal, such as wiping, degaussing, shredding, or incinerating, and that the process is effective and compliant with the organization's policies and standards. The other options are not as important as

verifying the vendor's process, because they either do not ensure the security and privacy of the information on the media, or they aresecondary to the vendor's process.
References: CISA Review Manual (Digital Version)1, Chapter 5, Section 5.2.7

NEW QUESTION: 618
□□□ □□□□□ □□ □□□□□□ □□□ □□ □□□ □□□ □□ □□□□ □ □□ □□ □□□ □□□ □□□□□?
A. □□ □□□ □□□□□ □□ □□□ □□□□□□□.
B. □□ □□ □□□ □□□□□ □□ □□□□□ □□□□□□□.
C. □□□□□□ □□□□ □□□□□.
D. □□□ □ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 619
□□ □ □□ □□ □□□□□ □□□□□ □□ □ □□□□ □□ □□□□□?
A. □□ □□ □□ □□
B. □□□ □□□ □□ □ □□
C. □□ □□□□ □□□□ □□ □□ □□□□□□.
D. IT □□□□ □□□ □□□□ □ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 620
□□ □ □□ □□□ □□□ □□ IT □□ □□□□ □□□ □□ IT □□ □□□□ □□□□ □□ □□ □□□□□ □□□□ □□ □□□ □□□□□□. □□ □ IS □□□□ □□ □□ □□ □□□ □□□□□?
A. IT □□□□□□ □□ □□□ □□□□□□□.
B. IT □□□□ □□□□□ □□□□□.
C. □□ □□ □□□ □□□□.
D. □□ IT □□□□□□ □□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 621
□□□ □□ 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: 622
□□ □□ □□□ □□ □□□ □□ □□□ □□ □□□□ □□ □□□ □□□□□ □□□.
A. □□ □□□ □□.
B. □□□□ □□.
C. □□ □□ □□.
D. □□□ □□□.
Answer: D (LEAVE A REPLY)
A proper audit trail of changes to server start-up procedures would include evidence of operator overrides, which are actions taken by the system operator to bypass or modify the normal execution of the server start-up process. Operator overrides may indicate unauthorized or improper changes that could affect the security, availability, or performance of the server. Therefore, an audit trail should capture and document any operator overrides that occur during the server start-up process.
Evidence of subsystem structure, program execution, and security control options are not directly related to changes to server start-up procedures. Subsystem structure refers to the components and relationships of a subsystem within a larger system. Program execution refers to the process of running a software program on a computer. Security control options refer to the settings and parameters that define the security level and access rights for a system or application. These are all important aspects of auditing a server, but they do not provide evidence of changes to server start-up procedures.

NEW QUESTION: 623
□□□ □□ □□□□ □□ □□ □□□ □□ □□□ □□□ □□□□□?
A. □□□
B. □□
C. □□
D. □□
Answer: B (LEAVE A REPLY)

Backup procedures for an organization's critical data are considered to be corrective controls, as they are designed to restore normal operations after a disruption or failure. Corrective controls aim to minimize the impact of an incident and prevent recurrence. Directive, detective and compensating controls are not related to backup procedures. Directive controls are intended to guide or instruct users to follow policies and procedures. Detective controls are intended to identify and report incidents or violations. Compensating controls are intended to mitigate the risk of a missing or ineffective primary control. References: CISA Review Manual (Digital Version), Chapter 2, Section 2.11

NEW QUESTION: 624
IT □□□□□ □□□ □□ □□□ □□ □□□□□ □□□.
A. □□□ □□□□□.
B. □□ □□ □□□.
C. □□ □ □□.
D. □□ □□.
Answer: (SHOW ANSWER)
IT governance should be driven by organizational strategies. It provides a formal structure for organizations to produce measurable results toward achieving their strategies and ensures that IT investments support business objectives12. While business unit initiatives, balanced scorecards, and policies and standards can play a role in IT governance, they are tools or methods that support the implementation of the organizational strategies.

NEW QUESTION: 625
□□ □ □□ □□ □□□□□ □□ □□□ □□□ □□□□□?
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: 626

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

A. □□□ □□□ □□□□□ □□□□□.

B. □□□ □□□ □□ □□□ □□□□ □□ □ □□□□.

C. □□□□□ □□□ □□□□ □□□ □□ □□ □□□□.

D. □□□□□ □□□ □□□ □ □□□□.

Answer: (SHOW ANSWER)

The main risk associated with adding a new system functionality during the development phase without following a project change management process is that the new functionality may not meet requirements (option B). This is because:

A project change management process is a set of procedures that defines how changes to the project scope, schedule, budget, quality, or resources are requested, evaluated, approved, implemented, and controlled12.

A project change management process helps to ensure that the changes are aligned with the project objectives, stakeholders' expectations, and business needs12.

Adding a new system functionality during the development phase without following a project change management process can introduce risks such as:

The added functionality has not been documented (option A), which can lead to confusion, inconsistency, errors, and rework3.

The project may fail to meet the established deadline (option C), which can result in delays, penalties, and customer dissatisfaction3.

The project may go over budget (option D), which can cause cost overruns, financial losses, and reduced profitability3.

However, the main risk is that the new functionality may not meet requirements (option B), which can have serious consequences such as:

The new functionality may not be compatible with the existing system or other components3.

The new functionality may not be tested or verified for quality, performance, security, or usability3.
The new functionality may not deliver the expected value or benefits to the users or customers3.
The new functionality may not comply with the regulatory or contractual obligations3.
The new functionality may cause dissatisfaction, complaints, or litigation from the stakeholders3.
Therefore, the main risk associated with adding a new system functionality during the development phase without following a project change management process is that the new functionality may not meet requirements (option B), as this can jeopardize the success and acceptance of the project.
References: 1: How to Make a Change Management Plan (Templates Included) - ProjectManager 2: What Is Change Management? Process & Models Explained - ProjectManager 3: 8 Steps for an Effective Change Management Process - Smartsheet

NEW QUESTION: 627
□□□ □□ □□□□ □□□□ □□□□. □□ □□□□ IT □□□ □□ □□□ □□□ □ □□□□ □□□□ □ □□ □□□□ □□□□□. □□ □□□ □□□ □□□□ □□□□?
A. □□□
B. □□
C. □□
D. □□
Answer: C (LEAVE A REPLY)
An organization is shifting to a remote workforce. In preparation, the IT department is performing stress and capacity testing of remote access infrastructure and systems. This type of control is being implemented to direct or guide actions to achieve a desired outcome. Therefore, it is a directive control. Directive controls are proactive controls that seek to prevent undesirable events from occurring. They include policies, standards, procedures, guidelines, training, and testing. Detective controls are reactive controls that seek to identify undesirable events that have already occurred. They include monitoring, logging, auditing, and reporting.
Preventive controls are proactive controls that seek to avoid undesirable events from occurring. They include authentication, encryption, firewalls, and antivirus software.
Compensating controls are alternative controls that provide a similar level of protection as the primary controls when the primary controls are not feasible or cost-effective. They include segregation of duties, manual reviews, and backup systems. References: CISA Review Manual (Digital Version), [ISACA Glossary of Terms]

NEW QUESTION: 628
□□ □ □□□ □□ □□□ □□□ □□□□ □ □□ □□□□ □□ □□□□□?
A. □□□□ □□□ □□□ □□□ □□□□.

B. □□□□ □□□□

C. □□□□ □□ □ □□□ □□□□□ □□□□□.

D. CCTV(□□□□□□□□)□ □□□□ □□□ □□□□□.

Answer: A (LEAVE A REPLY)

The most effective way for controlling visitor access to a data center is to ensure that visitors are escorted by an authorized employee, as this prevents unauthorized or malicious actions by the visitors and provides accountability and supervision. Pre-approval of entry requests, visitors signing in at the front desk upon arrival, and closed-circuit television (CCTV) are also useful measures, but they are not as effective as escorting visitors, as they do not prevent or detect unauthorized or malicious actions by the visitors in real time. References: CISA Review Manual (Digital Version), Chapter 5: Protection of Information Assets, Section 5.1: Physical Access Controls1